

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,

Petitioner,

v.

HEADWATER RESEARCH LLC,

Patent Owner.

Patent No. 8,023,425
Case No. IPR2026-00465

PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

I.	Introduction.....	1
II.	Technology Background.....	2
	1. Overview of <i>Thomas</i>	2
	2. Overview of <i>Buddhikot</i>	3
	3. Overview of <i>Haller</i>	4
	4. Overview of <i>Polson</i>	4
	5. Overview of <i>Weintraub</i>	5
III.	The '425 Patent.....	6
	A. Overview	6
	B. Prosecution History	7
IV.	Level of Ordinary Skill.....	8
V.	Claim Construction.....	8
VI.	Statement of Precise Relief Requested.....	8
	A. Ground 1: Claims 24, 25-32, 34, 36, 40-42, 44, 49, and 50 Are Obvious over <i>Thomas</i> and <i>Buddhikot</i>	10
	1. Motivation to Combine <i>Thomas</i> and <i>Buddhikot</i>	10
	a. Combining <i>Buddhikot</i> 's firewalling and packet- mangling policies with <i>Thomas</i> 's hotspot device	10
	b. Combining <i>Buddhikot</i> 's network congestion management scheme with <i>Thomas</i>	13
	2. Independent Claim 24	15

- a. 24[pre]: “A network system for activating an access network forwarding service for a first end point device,” 15
- b. 24[pre][i]: “the first end point device including an access network modem configured to communicate data over at least one access network, the access network modem providing a connection via at least one 2G, 3G or 4G wireless network;” 16
- c. 24[pre][ii]: “a local area network modem configured to communicate data with one or more additional end point devices over a local area network, the local area network modem providing a connection via at least one of Bluetooth, Wi-Fi or USB,” 19
- d. 24[pre][iii]: “a forwarding agent configured to forward the data between the access network modem and the local area network modem according to an access network forwarding policy to implement a network access forwarding service, the forwarding agent including a policy implementation agent configured to forward the data in the first end point device’s communications stack and including a firewall agent configured to pass or redirect the data to one or more specific access network routing paths according to the access network forwarding policy, and” 21
- e. 24[pre][iv]: “a service processor configured to” 24
- f. 24[pre][v]: “send one or more messages including information regarding a user response for activating the access network forwarding service to the network system,” 25
- g. 24[a]: “the network system comprising: one or more activation servers configured to:” 26
- h. 24[a][i]: “receive the one or more messages from the service processor of the first end point device, the one or more messages including information regarding the user response;” 28

- i. 24[a][ii]: “perform an activation sequence in response to receiving the information regarding the user response from the service processor; and” 28
- j. 24[a][iii]: “provision at least one of the first end point device and one or more network elements to allow the access network forwarding service to be provided on the first end point device; and.” 29
- k. 24[b]: “a service controller configured to:” 29
 - l. 24[b][i]: “obtain a service profile including one or more access network forwarding settings for the access network forwarding policy, the one or more access network forwarding settings including one or more restriction settings on the access network forwarding service, at least one of the access network forwarding settings identifying which access network route or traffic redirection is to be used by the first end point device when attempting to forward traffic between the one or more additional end point devices and the access network; and” 30
 - m. 24[b][ii]: “transmit the one or more access network forwarding settings to at least one selected from the group consisting of the first end point device and at least one of the one or more network elements.” 32
- 3. Claim 25: “The network system of claim 24, wherein the one or more messages includes credentials specific to the first end point device, and wherein the activation sequence is specific to the credentials.” 32
- 4. Claim 26: “The network system of claim 24, wherein a first activation server is configured to re-route the first end point device to a second activation server based on a credential received from the first end point device or based on a query-response sequence.” 33
- 5. Claim 27: “The network system of claim 24, wherein the one or more activation servers are further configured to

	provision the first end point device by transmitting software for updating the service processor of the first end point device.”	34
6.	Claim 28: “The network system of claim 24, wherein the one or more activation servers are operated by a virtual service provider, and wherein the virtual service provider bills a user of the first end point device for the access network forwarding service and provides a payment to a provider of the access network.”	35
7.	Claim 29: “The network system of claim 24, wherein the one or more network elements include at least one of an authentication and authorization server, a billing system, and one or more gateways.”	36
8.	Claim 30: “The network system of claim 29, wherein the service controller is further configured to assign the data to one or more specific access network routing paths.”	37
9.	Claim 31: “The network system of claim 24, wherein at least one of the one or more access network forwarding settings configures the forwarding agent to begin providing the forwarding of the data.”	38
10.	Claim 32: “The network system of claim 24, wherein at least one of the one or more access network forwarding settings is a function of a network congestion state.”	38
11.	Claim 34: “The network system of claim 24, wherein the one or more restriction settings includes a setting for enabling or disabling the access network forwarding service.”	40
12.	Claim 36: “The network system of claim 34, wherein a particular restriction setting is on a usage of a forwarding connection of the access network forwarding service, wherein the forwarding connection connects the one or more additional end point devices to the access network via the forwarding agent.”	40

13. Claim 40: “The network system of claim 24, wherein the service controller is further configured to provide a forwarding service notification to the first end point device or to an additional end point device during use of the access network forwarding service.” 41
14. Claim 41: “The network system of claim 40, wherein the forwarding service notification is provided when the access network forwarding service is enabled and the at least one access network includes a roaming access network.” 42
15. Claim 42: “The network system of claim 40, wherein the forwarding service notification informs the user of an amount of usage of the access network forwarding service, a rate of usage of the access network forwarding service, that the access network forwarding service is being used on a particular access network, that a service usage restriction setting is in place for the access network forwarding service, that the access network forwarding service is available or that the access network forwarding service is not available.” 43
16. Independent Claim 44 44
 - a. 44[pre]: “A method comprising:” 44
 - b. 44[a][i]: “receiving, at a service design system, first service plan elements of a first service plan for using an access network forwarding service, the access network forwarding service to be used by a first end point device,” 45
 - c. 44[b][i] “wherein the first service plan elements include one or more access network forwarding settings that define one or more restriction settings on the access network forwarding service, the one or more access network forwarding settings identifying which access network route or traffic redirection is to be used by the first end point device when attempting to forward traffic between the one or more additional end point devices and the access network;” 45

- d. 44[a][ii]: “the first end point device including an access network modem configured to communicate data over at least one access network, the access network modem providing a connection via at least one 2G, 3G or 4G wireless network, and” 48
 - e. 44[a][iii]: “a local area network modem configured to communicate data with one or more additional end point devices over a local area network, the local area network modem providing a connection via at least one of Bluetooth, Wi-Fi or USB;” 48
 - f. 44[b]: “generating an access network forwarding policy based on the first service plan elements, the access network forwarding policy defining a state of a forwarding connection, wherein the forwarding connection is configured to communicate the data between the one or more additional end point devices and the access network via the local area network modem and the access network modem,” 48
 - g. 44[c]: “associating the first end point device with the first service plan;” 50
 - h. 44[d]: “translating the access network forwarding policy to first instructions; and,” 51
 - i. 44[e]: “providing the first instructions to one or more policy implementation agents, the one or more policy implementation agents capable of implementing the access network forwarding policy for the first end point device.” 52
17. Claim 49: “The method of claim 44, wherein a particular restriction setting is on a usage of a forwarding connection of the access network forwarding service, wherein the forwarding connection connects the one or more additional end point devices to the access network via the forwarding agent.” 53

18.	Claim 50: “The method of claim 44, wherein the one or more policy implementation agents include the first end point device.”	53
B.	Ground 2: Claim 33 Is Obvious over <i>Thomas</i> , <i>Buddhikot</i> , and <i>Haller</i>	53
1.	Claim 33: “The network system of claim 24, wherein at least one of the one or more access network forwarding settings is a function of a time of day.”	53
C.	Ground 3: Claims 39, 43, and 45 Are Obvious over <i>Thomas</i> , <i>Buddhikot</i> , and <i>Polson</i>	56
1.	Motivation to combine <i>Thomas</i> , <i>Buddhikot</i> , and <i>Polson</i>	56
a.	Different settings for different access networks.....	57
b.	Restriction to a maximum number of additional end point devices.	59
2.	Claim 39: “The network system of claim 24, wherein the one or more access network forwarding settings includes at least one setting that is different for different access networks, each providing an access network forwarding service.”	60
3.	Claims 43 and 45:	62
a.	43: “The network system of claim 24, wherein a particular restriction setting restricts a forwarding connection of the network access forwarding service to a maximum number of additional end point devices, wherein the forwarding connection connects the one or more additional end point devices to the access network via the forwarding agent.”	62
b.	45: “The method of claim 44, wherein a particular restriction setting restricts use of the forwarding connection	

	of the network access forwarding service to a maximum number of additional end point devices.”	63
D.	Ground 4: Claims 35, 37, 38, 46, 47, and 48 Are Obvious over <i>Thomas, Buddhikot, and Weintraub</i>	64
1.	Motivation to combine <i>Thomas, Buddhikot, and Weintraub</i>	64
a.	Network traffic classification of the data	64
b.	Parental control policy	66
2.	Claims 35 and 48:	67
a.	Claim 35: “The network system of claim 34, wherein the one or more restriction settings includes restriction settings that vary depending on a network traffic classification of the data.”	67
b.	Claim 48: “The method of claim 44, wherein the one or more restriction settings include restriction settings that vary depending on a network traffic classification of the data.” 69	
3.	Claims 37, 38, 46, and 47	69
a.	Claim 37: “The network system of claim 24, wherein a particular restriction setting restricts data associated with certain network destinations from the access network forwarding service.”	69
b.	Claim 38: “The network system of claim 37, wherein the network destinations that are restricted are determined by a parental control policy.”	70
c.	Claim 46: “The method of claim 44, wherein a particular restriction setting restricts data associated with certain network destinations from the access network forwarding service.”	71

d.	Claim 47: “The method of claim 46, wherein the network destinations that are restricted are determined by a parental control policy.”.....	71
VII.	Mandatory Notices.....	72
A.	Real Parties-in-Interest.....	72
B.	Related Matters.....	74
C.	Lead and Back-Up Counsel.....	75
D.	Service Information.....	80
VIII.	Grounds for Standing.....	80
IX.	Conclusion	80

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	passim
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005) (en banc)	8

LIST OF EXHIBITS

<u>Exhibit</u>	<u>Description</u>
EX1001	U.S. Patent No. 8,023,425 to Raleigh (“the ’425 patent”).
EX1002	Prosecution History of U.S. Patent No. 8,023,425.
EX1003	Declaration of Bill Lin, Ph.D.
EX1004	Curriculum Vitae of Bill Lin, Ph.D.
EX1005	U.S. Patent Appl. Publ. No. 2009/0017789 to Thomas et al. (“ <i>Thomas</i> ”).
EX1006	Reserved
EX1007	Reserved
EX1008	Reserved
EX1009	Reserved
EX1010	Reserved
EX1011	Reserved
EX1012	Reserved
EX1013	U.S. Patent Appl. Publ. No. 2003/0035397 to Haller et al. (“ <i>Haller</i> ”).
EX1014	Reserved
EX1015	U.S. Patent Appl. Publ. No. 2007/0104169 to Polson (“ <i>Polson</i> ”) .
EX1016	U.S. Patent Appl. Publ. No. 2005/0102529 to Buddhikot et al. (“ <i>Buddhikot</i> ”).
EX1017	U.S. Patent Appl. Publ. No. 2008/0080493 to Weintraub et al. (“ <i>Weintraub</i> ”).

<u>Exhibit</u>	<u>Description</u>
EX1018	U.S. Patent Appl. Publ. No. 2010/0043068 to Varadhan et al. (“ <i>Varadhan</i> ”).
EX1019	Reserved.
EX1020	Reserved.
EX1021	Reserved.
EX1022	Reserved.
EX1023	Reserved.
EX1024	Reserved.
EX1025	<i>Headwater Research LLC v. Google LLC</i> , C.A. No. 3:26-cv-06230, Joint Claim Construction Statement, ECF No. 78 (W.D. Tex., June 5, 2026).

I. Introduction

Petitioner Google LLC respectfully requests *inter partes* review of claims 24-50 of U.S. Patent No. 8,023,425.

The '425 patent claims an end-user device capable of operating as an intermediate-networking device that communicates with a network system (e.g., the internet) over a wireless access network and provides a “forwarding service” to other devices (e.g., laptops), permitting them to communicate with the network system via the end-user device. The claimed end-user device implements conventional traffic-control service policies and user interfaces as were known in the art by January 28, 2009 (i.e., the earliest possible priority date). Specifically, the end-user device includes a forwarding agent comprising a policy implementation agent and a firewall agent configured to forward or redirect data flowing through the end-user device to various access-networking paths according to an access network forwarding policy.

These features, however, were well known. For example, *Thomas* and *Buddhikot* disclose all the features of independent claims 24 and 44. The dependent claims 25-43 and 45-50 recite other conventional hotspot features that a skilled artisan would have found obvious based on *Thomas*, *Buddhikot*, and one of *Haller*, *Polson*, or *Weintraub*.

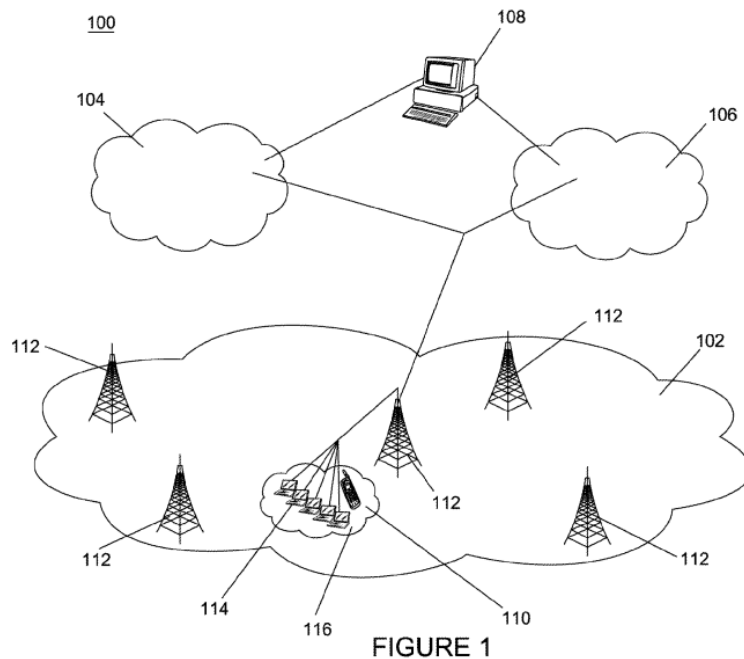
As detailed below and in the supporting declaration of Bill Lin, Ph.D., (EX1003), the challenged claims are unpatentable based on the grounds presented. EX1003, ¶¶6-7. The Board should institute review and cancel all challenged claims.

II. Technology Background

The following background discussion of the state of the prior art is based on Dr. Lin's testimony. EX1003, ¶¶39-49. Dr. Lin is a Professor of Electrical and Computer Engineering and the Associate Dean for Strategic Programs at the University of California, San Diego (UCSD). EX1003, ¶¶8-17. At UCSD, he is also a Principal Investigator in the UCSD Center for Networked Systems (CNS), where he contributes his expertise in the design of computer architecture solutions for wireless networking and mobile computing. EX1003, ¶12.

1. Overview of *Thomas*

Thomas discloses a network environment where “the wireless device 110 and the server 108, along with the WLAN 116, form an integrated networking capability for the client computing devices 114” that allows client computing devices 114 to “communicate normal traffic through the wireless device 110 to reach a network, such as the internet 104, or to access information on the server 108.” EX1005, ¶¶27, 47, Fig. 1; EX1003, ¶43.



EX1005, Fig. 1.

Thomas further discloses a message flow between wireless device 110 and server 107 “to configure the wireless device 110 for operation and to authorize the client computing device 114 for operation.” EX1005, ¶¶57-60, Fig. 7. As part of the “mobile, ad hoc point of presence” formed by wireless device 110, *Thomas* discloses an access network forwarding policy for metering usage and/or limiting number of concurrent users accessing the network through wireless device 110 (also referred to herein as *Thomas*’s hotspot device). EX1005, ¶¶46-47, 49-50, 54-55; EX1003, ¶44.

2. Overview of *Buddhikot*

Buddhikot discloses a gateway for mobile access. EX1016, ¶12. The gateway of *Buddhikot* includes a firewall service with firewalling and packet-

mangling rules to control data flow through its gateway. EX1016, ¶¶74, 76.

Buddhikot discloses that the firewall service “serve[s] the dual purpose of protecting the clients from malicious attacks coming from the Internet (such as PING floods, TCP syn floods, etc.), and of protecting the Gateway.” EX1016, ¶75.

Buddhikot’s packet-mangling rules provide “automatic redirection of user’s traffic.” EX1016, ¶76; EX1003, ¶45.

3. Overview of *Haller*

Haller discloses a “hand-held device for providing communication between a wide area network and a wireless local area network.” EX1013, ¶7. *Haller* discloses that “device 106 includes a display ... and a touchscreen, singly or in combination.” EX1013, ¶69. *Haller* discloses that its cellular phone hotspot device includes service level verification software that enforces service level agreements with users. EX1013, ¶¶54-56, 61, 140. *Haller* also discloses permitting unlimited amount of cellular traffic from its hotspot device during the night but limiting the traffic during the day. EX1013, ¶141; EX1003, ¶46.

4. Overview of *Polson*

Polson discloses a gateway adapted to establish a connection between itself and a WWAN with a WWAN interface adapted to receive data from and transfer data to the WWAN on behalf of devices of a LAN. EX1015, Abstract. *Polson* further discloses strategies for managing WWAN access, including adapting its

gateway to prioritize specific data over the WWAN to manage conflicts between end-user devices of LANs that are sharing limited WWAN capacity. EX1015, ¶46. *Polson* also recognizes that the mobility of its gateway is important and that the ability to connect to multiple WWANs is necessary when one WWAN is not available due to the location of the user, issues with the service provider, or the features of a service agreement. EX1015, ¶¶52-53; EX1003, ¶¶47-48.

5. Overview of *Weintraub*

Weintraub discloses parental control policies that prohibit a customer device within the customer's premises from accessing adult content from the external network. EX1017, ¶10. *Weintraub* also discloses different restriction settings based on a type of network content, for example, instant messaging or Voice over IP communications, peer-to-peer transmissions, e-mail transmissions, or streaming media. EX1017, ¶26. *Weintraub* discloses restricting forwarding of data based on source or destination, time of day, attachments, or type of content. *Id.*, EX1003, ¶49.

III. The '425 Patent

The '425 patent was filed on March 2, 2009, and claims priority to a provisional application filed January 28, 2009.¹ EX1001, cover.

A. Overview

The '425 patent discloses a system that allows an end-user device to be used as an intermediate networking device. EX1001, 32:34-44, 35:21-29. Figure 15 reflects the purported invention:

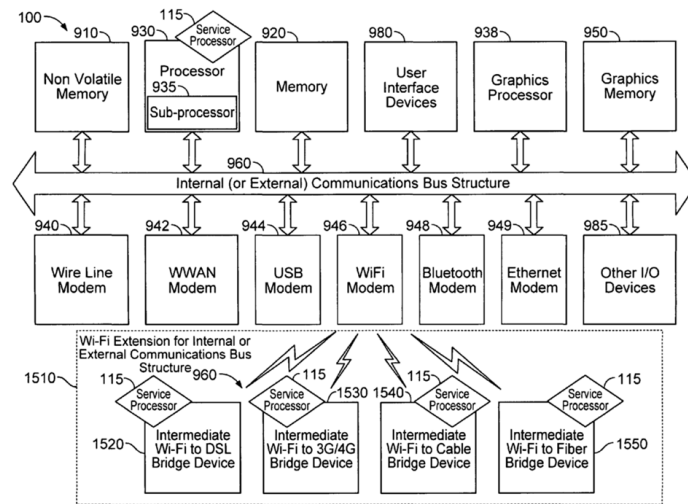


FIG. 15A

EX1001, Fig. 15A. The end-user device includes a modem. The memory stores service-policy settings for authorizing the end-user device to provide a forwarding service. The service processor obtains configuration information, obtains a user

¹ Petitioner reserves the right to challenge the priority date if Patent Owner attempts to antedate any of the prior art.

input through a user interface, and modifies a service-policy setting to enable or disable the forwarding service. EX1003, ¶41.

B. Prosecution History

During prosecution, the Examiner issued one office action which rejected application claim 21 under 35 U.S.C. § 101 and rejected application claims 1-8, 21, and 22 on the ground of non-statutory double patenting over co-pending U.S. Application No. 12/380,769. EX1002, 241-251. The Examiner also rejected application claims 1-4, 9-11, 21, and 22 as anticipated by *Varadhan* (EX1018). In response, Applicant cancelled application claims 1-22 and presented new claims 23-77. EX1002, 120-130. The Examiner issued a Notice of Allowance, cancelling application claims 29, 30, and 35, adding the subject matter of these claims to the independent claims, and allowing the remaining application claims. EX1002, 77-95. In the reasons for allowance, the Examiner stated:

[The claims] are allowed over the prior art of record since the cited references taken individually or in combination fails to particularly disclose **the forwarding agent including a policy implementation agent configured to forward the data in the first end point device's communications stack, and a firewall agent configured to pass or redirect the data to one or more specific access network routing paths according to the access network forwarding policy.**

EX1002, 95 (emphasis in original). The Examiner, however, erred in allowing the claims over clear teachings in the prior art disclosing the claimed “forwarding agent,” as discussed in this Petition below. EX1003, ¶42.

IV. Level of Ordinary Skill

A person of ordinary skill in the art (“POSITA”) at the ’425 patent’s effective filing date would have at least a bachelor’s degree in computer science, electrical engineering, or a related field, and at least two years of work/research experience in the field of computer networking and networking devices. EX1003, ¶51. More related education would compensate for fewer years of work experience (and vice versa). EX1003, ¶51.

V. Claim Construction

Claims in an IPR are construed under *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). 37 C.F.R. § 42.100(b). For purposes of this Petition, no terms need to be expressly construed. EX1025. Petitioner reserves the right to respond to any claim-construction arguments raised by the Patent Owner.

VI. Statement of Precise Relief Requested

Petitioner requests review under 35 U.S.C. § 311 of claims 24-50 of the ’425 patent and cancellation of those claims as obvious under pre-AIA 35 U.S.C. § 103 based on the following unpatentability grounds.

	References	Basis	Challenged Claims
1	<i>Thomas and Buddhikot</i>	§ 103	Claims 24, 25-32, 34, 36, 40-42, 44, 49, and 50
2	<i>Thomas and Buddhikot</i> in view of <i>Haller</i>	§ 103	Claim 33
3	<i>Thomas and Buddhikot</i> in view of <i>Polson</i>	§ 103	Claims 39, 43, and 45
4	<i>Thomas and Buddhikot</i> in view of <i>Weintraub</i>	§ 103	Claims 35, 37, 38, 46, 47, and 48

The '425 patent claims priority to multiple provisional applications, the earliest of which was filed January 28, 2009. EX1001, Cover. All references asserted in this Petition qualify as prior art under pre-AIA 35 U.S.C. § 102(a), (b), and/or (e) even if January 28, 2009, is used as the priority date of the '425 patent:

EX1005	U.S. Patent Publication 2009/0017789 (" <i>Thomas</i> "), filed January 22, 2008, published January 15, 2009; prior art under §§ 102(a), (e).
EX1013	U.S. Patent Publication 2003/0035397 (" <i>Haller</i> "), filed Aug. 17, 2001, issued Nov. 13, 2007; prior art under §§ 102(a), (b), (e).
EX1015	U.S. Patent Publication 2007/0104169 (" <i>Polson</i> "), filed Nov. 10, 2006, published May 10, 2007; prior art under §§ 102(a), (b), (e).
EX1016	U.S. Patent Publication 2005/0102529 (" <i>Buddhikot</i> "), filed Oct. 20, 2003, published May 12, 2005; prior art under §§ 102(a), (b), (e).
EX1017	U.S. Patent Publication 2008/0080493 (" <i>Weintraub</i> "), filed Sep. 29, 2006, published Apr. 3, 2008; prior art under § 102(a), (e).

A. Ground 1: Claims 24, 25-32, 34, 36, 40-42, 44, 49, and 50 Are Obvious over *Thomas* and *Buddhikot*

1. Motivation to Combine *Thomas* and *Buddhikot*

Thomas and *Buddhikot* are analogous art to the '425 patent because they are in the same field of endeavor: mobile devices and wireless access points for computer networking. EX1005, ¶¶2, 6, 9, 23, 28, 84-85, Figs. 1-11; EX1016, Abstract, ¶¶2, 32, 45-47, 52-53, 182-189, Figs. 1-15; EX1001, 32:34-35:20. They also share a common goal with the '425 patent: using end-user devices for bridging or routing traffic from other devices to a network system (e.g., the internet), including the provisioning of services seeking to improve the customizability and monetization of mobile-hotspot technology (e.g., usage control, user interactivity and notifications via graphical user interfaces, and billing features). EX1005, ¶¶23, 28, 44-45, 54-55, 79-80; EX1016, Abstract, ¶¶2, 32, 45-47, 52-53, 182-189; EX1001, 32:34-35:20, 65:31-67, Figs. 15A-F; EX1003, ¶53.

a. Combining *Buddhikot*'s firewalling and packet-mangling policies with *Thomas*'s hotspot device

Thomas discloses controlling traffic flow through wireless device 110—a hotspot device—and discloses a firewall configured to operate on the hotspot device. EX1005, ¶¶42, 54, 69. *Buddhikot* discloses a firewall service with firewalling and packet-mangling rules to control data flow through its gateway. EX1016, ¶¶74, 76, 114. A POSITA would have been motivated to implement

Buddhikot's firewall and packet-mangling rules on *Thomas*'s hotspot device because doing so would have provided a more refined way to control network traffic through *Thomas*'s hotspot device. EX1003, ¶54.

For example, *Buddhikot* discloses two benefits of its firewall service. EX1016, ¶¶75-76. First, *Buddhikot*'s firewalling rules protect both *Buddhikot*'s gateway and the client devices connected to the gateway from malicious attacks. EX1016, ¶75; EX1003, ¶55. Second, *Buddhikot*'s packet-mangling rules for redirecting traffic to a local web cache help reduce network traffic flowing to the access network. EX1016, ¶76; EX1003, ¶55. A POSITA would have been motivated to implement *Buddhikot*'s access network forwarding policy (including firewall and packet-mangling rules) on *Thomas*'s hotspot device to obtain these same benefits. EX1003, ¶55. The implementation of *Buddhikot*'s firewalling and packet-mangling rules on *Thomas*'s hotspot device would have been nothing but a combination of familiar elements (e.g., firewalling and packet-mangling rules on a gateway) according to known methods (e.g., implementing the rules to forward or redirect data flowing through the gateway) to obtain predictable results (e.g., protecting devices from malicious attacks and reducing network traffic by redirection to the local DNS or web cache). EX1003, ¶55; *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007).

A POSITA would have had a reasonable expectation of success in implementing *Buddhikot*'s QoS and firewall rules on *Thomas*'s hotspot device. *Thomas* already discloses using rules to meter usage, limit the number of concurrent connections, and allow data to flow through its hotspot device based on a desired service level. EX1005, ¶¶46-47, 49-50, 54-55. *Thomas* also discloses a firewall that may be implemented on its hotspot device. EX1005, ¶42. *Buddhikot* discloses how to implement the QoS, firewall, and packet-mangling rules to control the flow of data through a gateway device. EX1016, ¶¶74, 76, 114. Because *Thomas* already discloses the use of rules, implementing *Buddhikot*'s QoS, firewall, and packet-mangling rules on *Thomas*'s hotspot device would have involved known techniques as disclosed by *Thomas* and *Buddhikot* and would have been well within the skill level of a POSITA. EX1003, ¶56. Accordingly, a POSITA would have had a reasonable expectation of success in combining *Buddhikot*'s teachings with *Thomas*. *KSR*, 550 U.S. at 421; EX1003, ¶56.

A POSITA would have also been motivated to modify *Thomas*'s server using *Buddhikot*'s teachings so that the modified *Thomas-Buddhikot* server provides *Buddhikot*'s firewalling and packet-mangling rules to *Thomas*'s hotspot device. EX1003, ¶57. A POSITA would have done so to obtain the same benefits of protecting devices from malicious attacks and reducing network traffic by redirection to the local DNS or web cache as discussed above. EX1003, ¶57.

A POSITA would have had a reasonable expectation of success in modifying *Thomas*'s server to implement *Buddhikot*'s firewalling and packet-mangling rules. EX1003, ¶58. *Thomas* already discloses that its server provides rules to meter usage, limit the number of concurrent connections, and allow data to flow through its hotspot device based on a desired service level. EX1005, ¶¶46-47, 49-50, 54-55. *Thomas* also discloses that a firewall may be configured to operate on its server. EX1005, ¶42. Thus, modifying *Thomas*'s server to also provide *Buddhikot*'s firewall and packet-mangling rules to *Thomas*'s hotspot device would have been a combination of familiar elements (e.g., rules) according to known methods (e.g., providing rules from a server) to obtain predictable results (e.g., a modified server capable of providing a variety of rules to hotspot devices). EX1003, ¶58; *KSR*, 550 U.S. at 416, 421.

b. Combining *Buddhikot*'s network congestion management scheme with *Thomas*

Thomas discloses an access network forwarding policy for metering usage and/or limiting the number of concurrent users. EX1005, ¶¶46-47, 49-50, 54-55. *Buddhikot* discloses guaranteeing a minimum bandwidth to client devices connected to its gateway. EX1016, ¶78. *Buddhikot* also discloses adjusting the bandwidth provided to client devices when network congestion occurs, for example, by reducing bandwidth for all connected client devices instead of

allowing some users to use all the bandwidth and blocking other users completely. EX1016, ¶78. *Buddhikot* explains that its approach is based on fairness to allow all users to access the network. EX1016, ¶78. A POSITA would have found it obvious to combine the access network forwarding policy of *Thomas* with the network congestion management scheme of *Buddhikot*. EX1003, ¶59.

A POSITA would have been motivated to implement *Buddhikot*'s congestion management scheme on *Thomas*'s hotspot device because doing so would ensure client end point devices connected to the access network through *Thomas*'s hotspot device are able to exchange data with the access network instead of being disconnected. A POSITA would have been motivated to do so to ensure fairness for all connected client devices and to improve the user experience and satisfaction with the forwarding service provided by the *Thomas-Buddhikot* hotspot device. EX1003, ¶60. The implementation of *Buddhikot*'s congestion management QoS rules on *Thomas*'s hotspot device would have been nothing but a combination of familiar elements (e.g., known QoS rules) according to known methods (e.g., implementing the QoS rules to forward or redirect data flowing through the gateway) to obtain predictable results (e.g., ensuring connected devices can exchange data with the access network even in the face of network congestion). EX1003, ¶60; *KSR*, 550 U.S. at 416. As also discussed, a POSITA would have had a reasonable expectation of success in combining *Buddhikot*'s QoS rules with

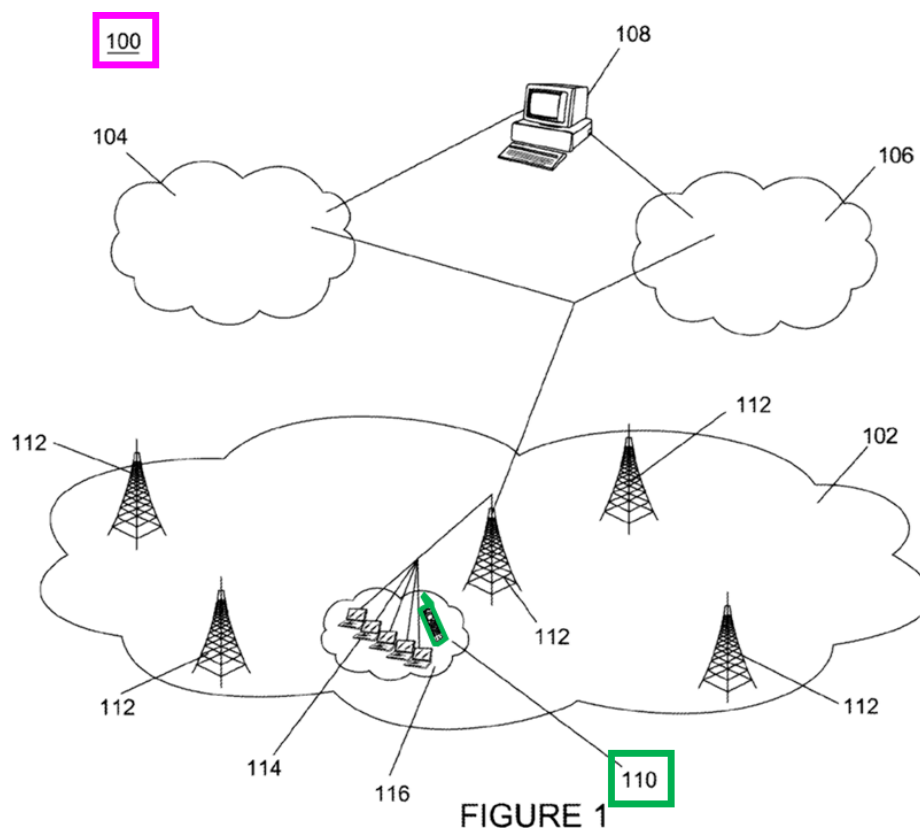
Thomas because implementing rules was already taught by both *Thomas* and *Buddhikot*. *Supra* §VI.A.1.a.

2. Independent Claim 24

The *Thomas-Buddhikot* combination discloses claim 24. EX1003, ¶¶61.

a. 24[pre]: “A network system for activating an access network forwarding service for a first end point device,”

Thomas discloses 24[pre]. EX1003, ¶¶62. *Thomas* discloses a network environment 100 including wireless device 110, client devices 114, server 108, and cellular network 102 that connects to internet 104. EX1005, ¶¶24-25, Fig. 1.



EX1005, Fig. 1 (annotated).

Thomas's "wireless device 110 forms a mobile, ad hoc point of presence within the cellular network for the client computing devices 114." EX1005, ¶27; *see also id.*, ¶¶25, 16, 47. According to *Thomas*, "the wireless device 110 and the server 108, along with the WLAN 116, form an integrated networking capability for the client computing devices 114." EX1005, ¶27. Further, "the client computing device 114 is allowed to communicate normal traffic through the wireless device 110 to reach a network, such as the internet 104, or to access information on the server 108." EX1005, ¶47. The server 108 of network system 100 configures the wireless device 110 for operation. EX1005, ¶57. Thus, *Thomas*'s network environment 100 (e.g., "network system") is configured to activate wireless device 110 (e.g., "first end point device") for communication of traffic (e.g., "access network forwarding service") from client devices 114 through cellular network 102 to internet 104 through wireless device 110 (e.g., access network). EX1003, ¶63.

b. 24[pre][i]: "the first end point device including an access network modem configured to communicate data over at least one access network, the access network modem providing a connection via at least one 2G, 3G or 4G wireless network;"

Thomas discloses 24[pre][i]. EX1003, ¶¶64. *Thomas*'s wireless device 110 includes a radio frequency front-end 300 that "provides radio frequency (RF) control and signaling capabilities for bi-directional communication for the wireless

device 110.” EX1005, ¶33. *Thomas’s* DSP 304 converts the signal from analog to digital (or vice versa) and “modulates and demodulates data to process signaling received from or transmitted to the RF front-end 300.” EX1005, ¶33.

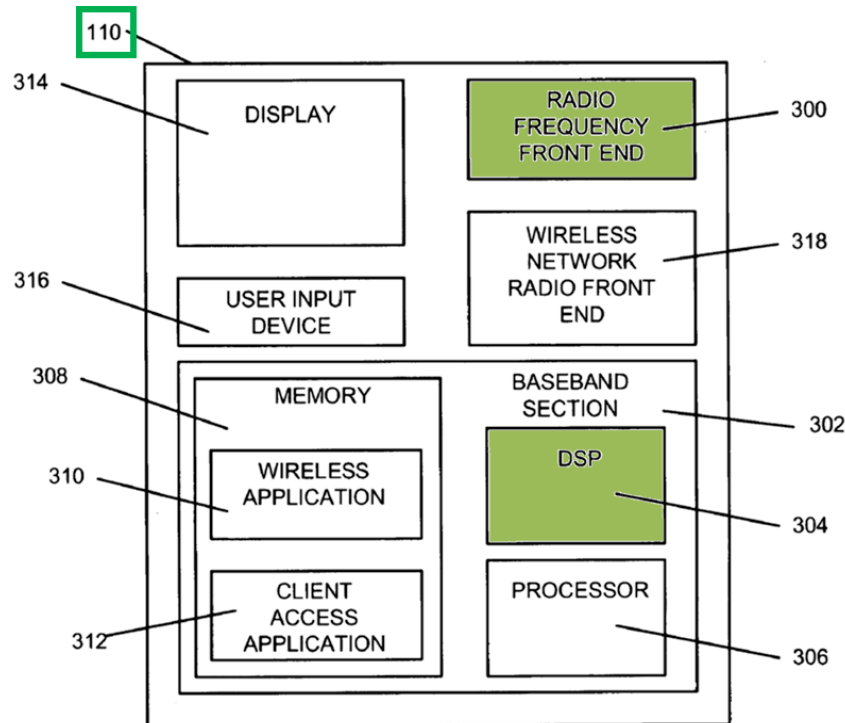
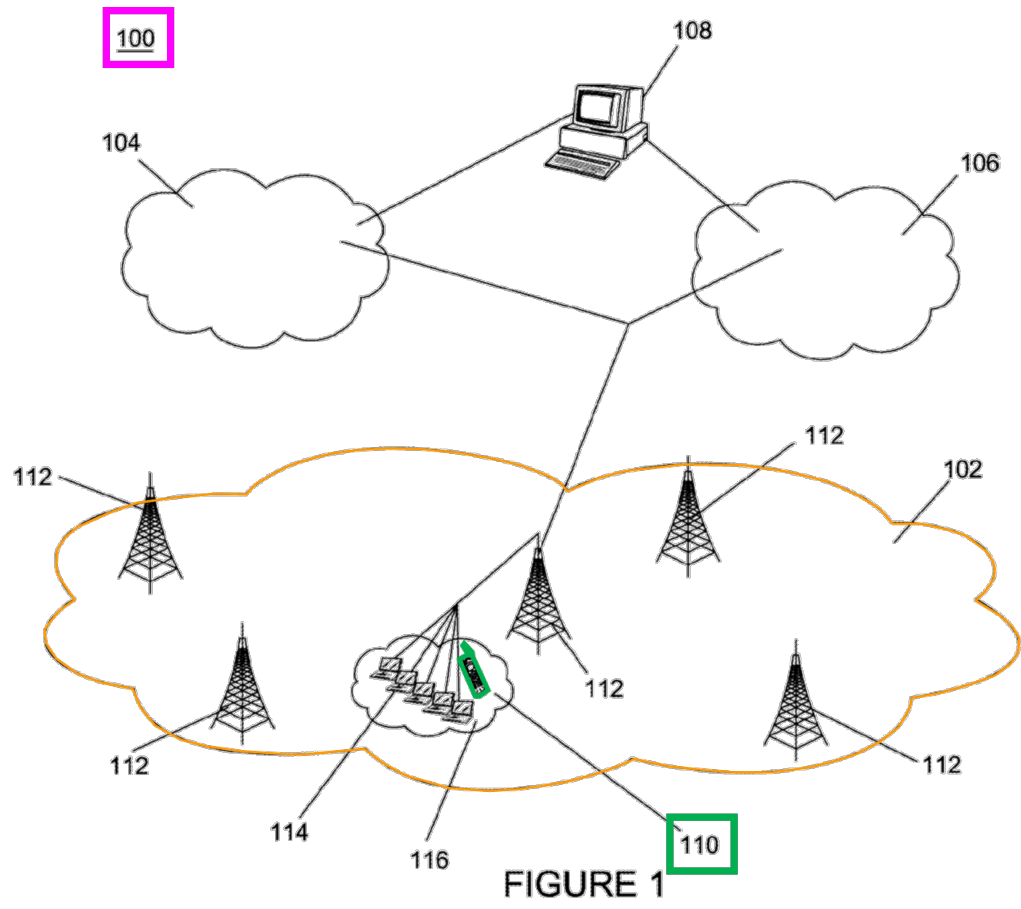


FIGURE 3

EX1005, Fig. 3 (annotated).

Thomas’s cellular network 102 “provides voice and data services to a wireless device 110 via wireless signals, such as wireless signals based on well established world wide standard transmission formats (e.g., GSM, CDMA, W-CDMA, UMTS, WiMAX, etc.) or any other wireless signals.” EX1005, ¶25, Fig. 1.



EX1005, Fig. 1 (annotated). *Thomas* discloses that **wireless device 110** “may utilize any cellular data network technology (e.g., 2.5G, 3G, 4G, or any future technology).” EX1005, ¶32. Thus, *Thomas*’s wireless device 110 includes a **radio frequency front-end 300** and **DSP 304** (i.e., “**access network modem**”) that communicates data over **cellular network 102** (i.e., “**access network**”) via at least a 3G or 4G wireless network as claimed. EX1003, ¶65.

c. 24[pre][ii]: “a **local area network modem** configured to communicate data with **one or more additional end point devices** over a **local area network**, the **local area network modem** providing a connection via at least one of **Bluetooth, Wi-Fi or USB,**”

Thomas discloses 24[pre][ii]. EX1003, ¶¶66. Thomas discloses a **wireless network radio front end 318** that “provides communication capabilities for the **wireless device 110.**” EX1005, ¶34.

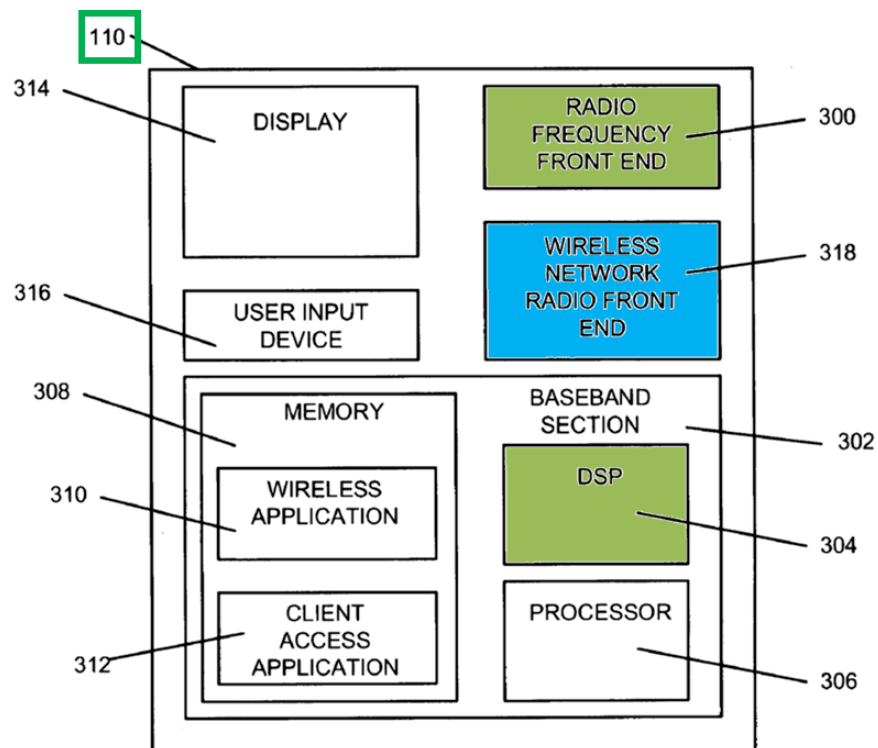
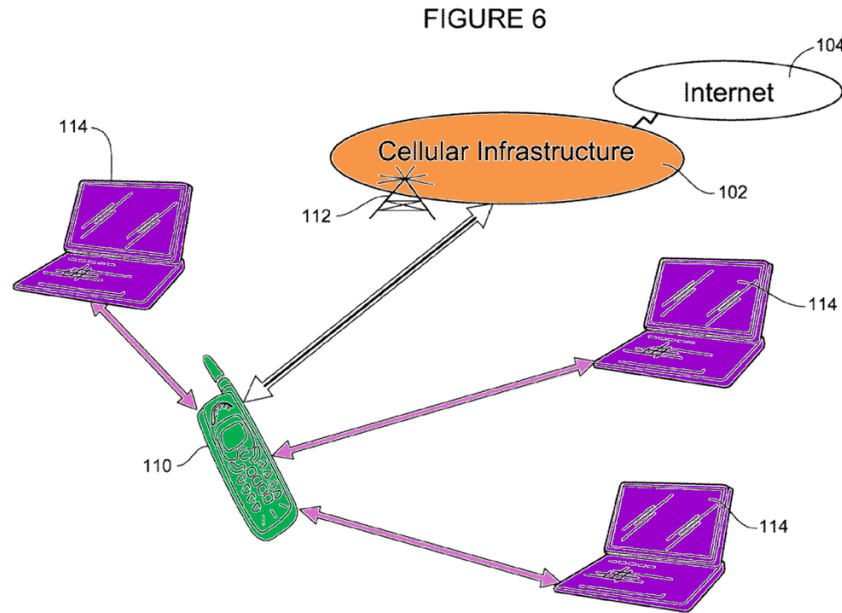


FIGURE 3

EX1005, Fig. 3. Thomas’s wireless device 110 also includes “processor 306,” which “is further adapted to communicate via the wireless network radio front end with the at least one computing device.” EX1005, ¶33, claim 7. Thus, as shown below, Thomas’s **wireless device 110** “provid[es] data services to **client computing**

devices 114 via a shorter range wireless local area network (WLAN) 116” using, for example, 802.11 WLAN. EX1005, ¶¶25-26, Fig. 6.



EX1005, Fig. 6 (annotated). *Thomas* therefore discloses that the wireless network radio front end communicates with at least one computing device to provide access to network infrastructure. EX1005, claim 7. Accordingly, *Thomas*’s wireless device 110 includes a wireless network radio front end 318 (e.g., “local area network modem”) that communicates data over 802.11 WLAN 116 (e.g., “local area network”) via Wi-Fi. EX1003, ¶66.

d. 24[pre][iii]: “a forwarding agent configured to forward the data between the **access network modem** and the **local area network modem** according to an access network forwarding policy to implement a **network access forwarding service**, the forwarding agent including a **policy implementation agent** configured to forward the data in the first end point device’s communications stack and including a **firewall agent** configured to pass or redirect the data to one or more specific access network routing paths according to the access network forwarding policy, and”

The *Thomas-Buddhikot* combination discloses 24[pre][iii]. EX1003, ¶67.

Thomas’s **client-access application 312** and **associated software** are a “**policy implementation agent**,” which together with *Thomas*’s **firewall** (i.e., “**firewall agent**”) constitute the claimed “forwarding agent.” *Thomas* discloses that software running on wireless device 110 distributes data services offered by cellular network 102 in local area networks (LAN) supported by 802.11. EX1005, ¶30; EX1003, ¶67.

Thomas discloses a “client-access application 312” providing “application-level point-of-presence capabilities within wireless device 110”. EX1005, ¶34. This **client-access application** and **its associated software** forward data in *Thomas*’s wireless-device-communication stack by forwarding data from client-computing device 114 through wireless device 110 to reach internet 104. EX1005, ¶¶27, 46, 47, 84, 85, EX1003, ¶¶67-68. Further, *Thomas* discloses a **firewall** (i.e., “**firewall**

agent”) configured to operate on either the wireless device 110 or the server 108.

EX1005, ¶42.

This forwarding agent in Thomas is “configured to forward the data between the access network modem and the local area network modem . . . to implement a network access forwarding service.” *Thomas*’s wireless-network-radio front end 318 (i.e., “local area network modem”) communicates data with client-computing devices 114, and *Thomas*’s radio-frequency front-end 300 and DSP 304 (i.e., “access network modem”) communicates with cellular network 102. EX1005, ¶¶25, 32-34, Figs. 3, 6; *supra* §§VI.A.2.b, VI.A.2.c. *Thomas*’s forwarding agent (i.e., client-access application, its associated software, and firewall) forwards data through between *Thomas*’s wireless-network-radio front end 318 (i.e., “local area network modem”) and *Thomas*’s radio-frequency front-end 300 and DSP 304 (i.e., “access network modem”). Forwarding data in this manner constitutes implementing a network access forwarding service. EX1003, ¶68.

Thomas also discloses forwarding such data according to an “access network forwarding policy.” *Thomas* discloses metering usage based on time duration of connection, number and size of packets sent or received, or QoS requirements. EX1005, ¶54. *Thomas* discloses that a number of concurrent users may be controlled based on a “service level” for the client access application 312. EX1005, ¶69. Metering usage based on service-level or QoS, and controlling number of

concurrent users constitutes applying settings associated with an access-network-forwarding policy. EX1003, ¶69.

Thomas discloses a firewall, but does not explain explicitly how its firewall forwards or redirects data. *Buddhikot* discloses these features. *Buddhikot* discloses a gateway that provides data communication between a 3G cellular-access network and devices connected to the gateway via a LAN. EX1016, ¶¶12, 32, 34, 41-42. Like *Thomas*, *Buddhikot*'s gateway provides QoS services, including providing guaranteed bandwidth and adjusting bandwidth if there are too many users connected to the gateway. EX1016, ¶¶46, 78-81, 176-179. Further, *Buddhikot*'s gateway supports a dynamic-stateful-firewall service. EX1016, ¶74. *Buddhikot*'s firewall service implements firewalling rules for protecting clients from malicious attacks from the internet and protecting *Buddhikot*'s gateway against traffic from malicious clients. EX1016, ¶75; EX1003, ¶70.

Buddhikot's firewall service also implements packet-mangling rules for automatic redirection of user's traffic (i.e., data received from client devices connected to the gateway) to local services, such as a local DNS server or a web-cache. EX1016, ¶76. *Buddhikot* explains that a user's web requests to a web server 305 get redirected to the cache 304. EX1016, ¶113. When the cache does not have the requested information (i.e., cache miss), the requests are forwarded to a web server on the internet. *Id.* Conversely, if the cache has the requested information

(i.e., cache hit), that information is provided without forwarding the data to the web server. *Id.* Thus, *Buddhikot*'s firewall service either forwards the data or redirects the data according to specific network routing paths (e.g., path to web server or path to local DNS server or cache) based on its packet-mangling rules. EX1003, ¶71. A POSITA would have found it obvious to implement *Buddhikot*'s QoS, firewalling, and packet-mangling functionality on *Thomas*'s hotspot device and would have had a reasonable expectation of success in doing so. *Supra* §VI.A.1; EX1003, ¶¶71-72.

Thomas modified with *Buddhikot*'s firewall service details (hereafter, the “*Thomas-Budhhikot* hotspot device”) renders obvious the forwarding agent of 24[pre][iii]. EX1003, ¶72.

e. 24[pre][iv]: “a service processor configured to”

Thomas discloses 24[pre][iv]. EX1003, ¶¶73. *Thomas*'s wireless device 110 includes “processor 306,” (e.g., “service processor”) that “provides computational and processing capabilities for the wireless device 110 and includes signal processing capabilities.” EX1005, ¶33, Fig. 3. Processor 306 is a “service processor” because it provides processing capabilities to implement the network-access-forwarding service. EX1003, ¶73.

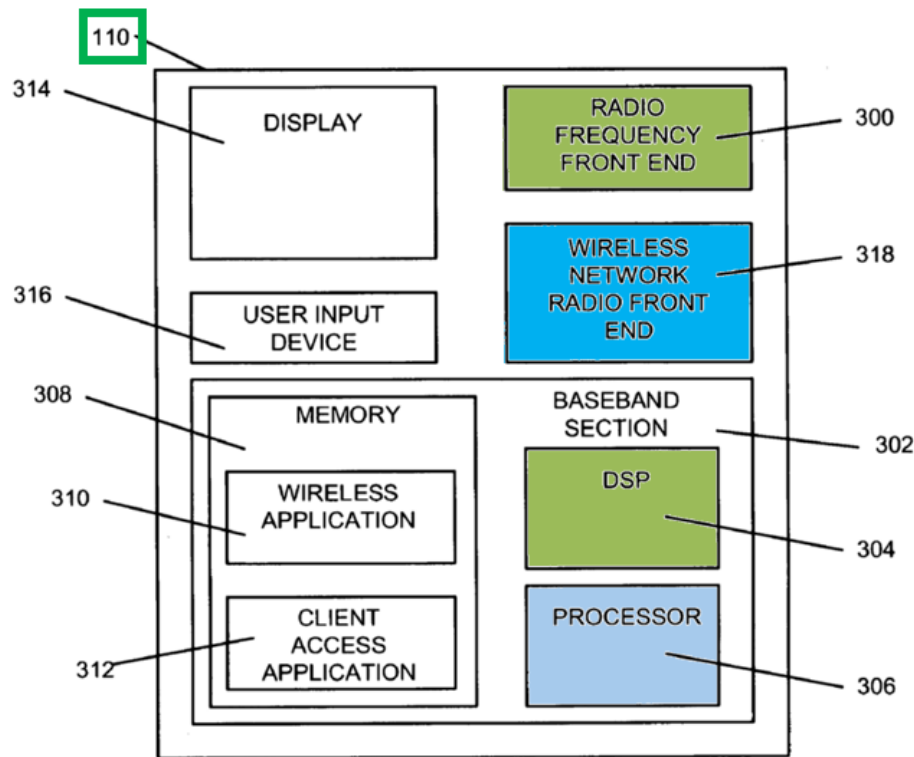


FIGURE 3

EX1005, Fig. 3 (annotated).

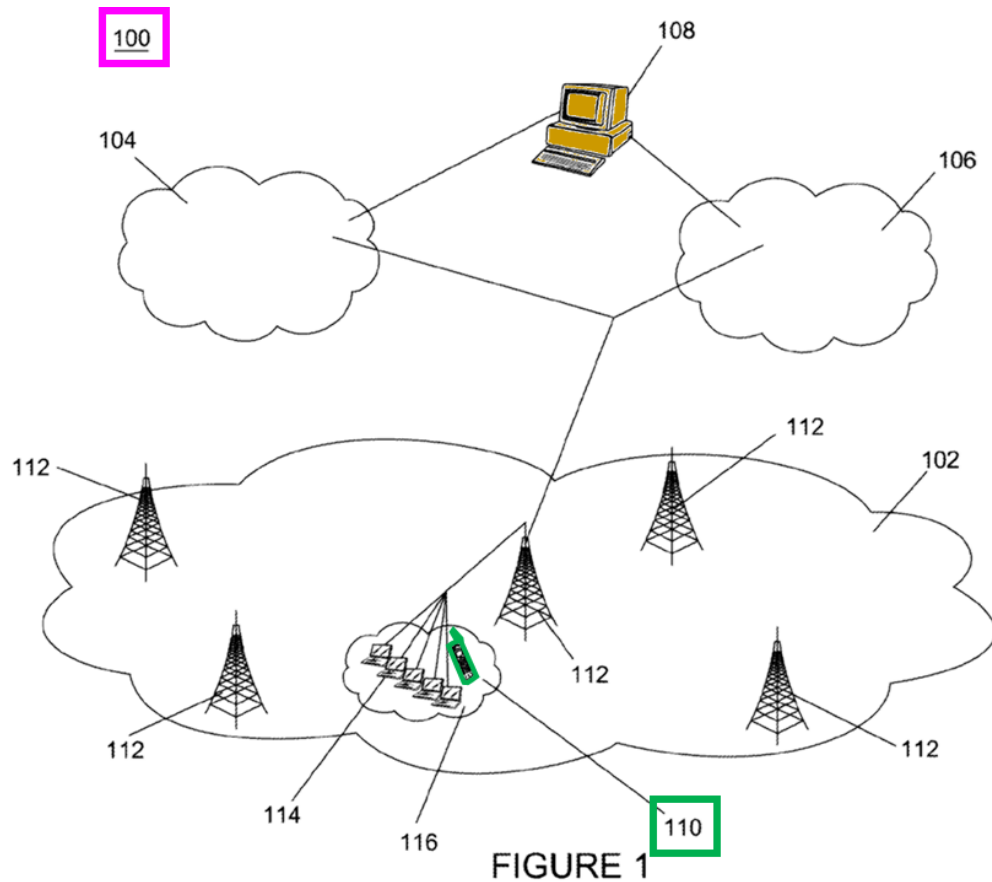
f. 24[pre][v]: “send one or more messages including information regarding a user response for activating the access network forwarding service to the network system,”

Thomas discloses 24[pre][v]. EX1003, ¶¶74. According to *Thomas*, “[w]hen the user of the wireless device 110 starts the client access application 312, a start message is sent from the wireless device 110 to the server 108.” EX1005, ¶58, Fig. 7. Starting the client access application 312 is a user response requesting activation of *Thomas*’s hotspot device. EX1003, ¶74. For example, the start message “includes parameters, such as message type, phone international mobile equipment identification (IMEI), cell identifier, software version, and comments.” EX1005,

¶62. Thus, *Thomas*'s hotspot device sends the start message (e.g., "one or more messages") including various parameters (e.g., "information regarding a user response") to server 108, which is part of *Thomas*'s network system 100. EX1003, ¶74; *supra* §VI.A.1.g. A POSITA would have understood that processor 306 of *Thomas*'s hotspot device would have caused the start message to be sent to server 108 because "processor 306 provides computational and processing capabilities for the wireless device 110 and includes signal processing capabilities to perform signal and channel correlations." EX1005, ¶33; EX1003, ¶74.

**g. 24[a]: "the network system comprising: one or more
activation servers configured to:"**

Thomas discloses 24[a]. EX1003, ¶75. In *Thomas*'s network 100, "cellular (telephone) network 102 connects via an Internet 104 connection . . . to a server 108." EX1005, ¶24.



EX1005, Fig. 1. “In response to determining whether the **wireless device 110** is authorized, the **server 108** sends a start response message (line 2) to the requesting **wireless device 110**.” EX1005, ¶59. Thus, *Thomas’s* **server 108** is an activation server as claimed because it allows **wireless device 110** to become activated to provide services to other client devices. EX1003, ¶75.

h. 24[a][i]: “receive the one or more messages from the service processor of the first end point device, the one or more messages including information regarding the user response;”

Thomas discloses 24[a][i]. EX1003, ¶¶76. *Thomas*’s activation server 108 receives a start message (e.g., “one or more messages”), including one or more parameters (e.g., “information regarding the user response”) from processor 306 (e.g., “service processor”) of *Thomas*’s hotspot device (e.g., “first end point device”). *Supra* §VI.A.2.f.; EX1003, ¶76.

i. 24[a][ii]: “perform an activation sequence in response to receiving the information regarding the user response from the service processor; and”

Thomas discloses 24[a][ii]. EX1003, ¶¶77. *Thomas* discloses that server 108 determines whether a requesting device is authorized to operate within *Thomas*’s network after receiving a start message from the wireless device. EX1005, ¶59. “In response to determining whether the wireless device 110 is authorized, the server 108 sends a start response message (line 2) to the requesting wireless device 110.” EX1005, ¶59, Fig. 7. By determining whether wireless device 110 is authorized to operate in the network and sending a start response message, *Thomas*’s server 108 performs an activation sequence permitting *Thomas*’s hotspot device to act as an ad hoc point of presence device. EX1003, ¶77.

j. 24[a][iii]: “provision at least one of the first end point device and one or more network elements to allow the access network forwarding service to be provided on the first end point device; and.”

Thomas discloses 24[a][iii]. EX1003, ¶78. *Thomas* discloses providing a service level and parameters such as “number of available IP addresses, base IP address, lease time, short lease time, . . . data amount remaining, byte count on/off, [and] port restriction on/off” to *Thomas*’s hotspot device (the first end point device). EX1005, ¶59. By providing this information to *Thomas*’s hotspot device, server 108 in *Thomas*’s network system 100 provisions *Thomas*’s hotspot device to allow the access network forwarding service. EX1005, ¶59; EX1003, ¶78; EX1001, 120:66-121:3 (“provisioning includes assigning, programming or embedding into the device . . . level of service activity, referred to as service profile.”).

k. 24[b]: “a service controller configured to:”

Thomas discloses 24[b]. EX1003, ¶79. *Thomas*’s server 108 includes processor 402, which is a service controller that “provides computational and processing capabilities for the server 108.” EX1005, ¶38, Fig. 4; *compare with* EX1001, 16:9-22 (“[N]etwork control of the service policy settings and services as discussed above is accomplished with the service controller 122 which in various embodiments includes one or more server functions.”); EX1003, ¶79.

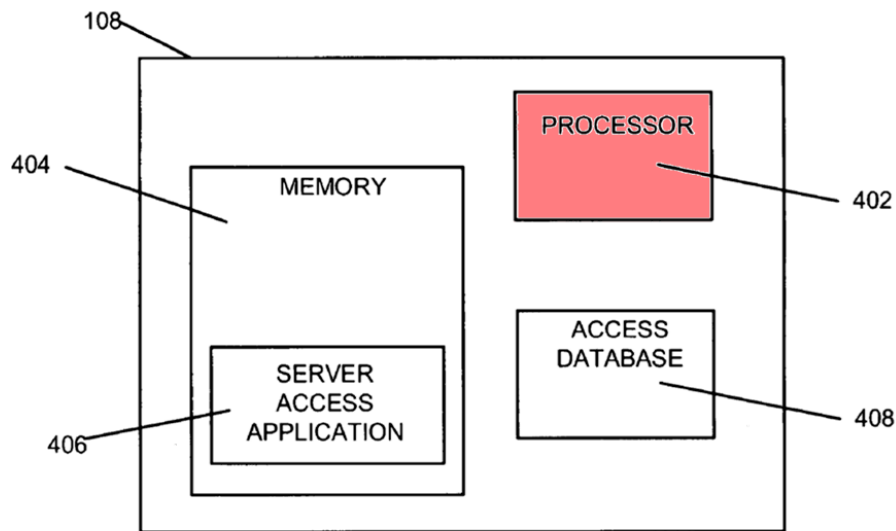


FIGURE 4

EX1005, Fig. 4 (annotated).

I. 24[b][i]: “obtain a service profile including one or more access network forwarding settings for the access network forwarding policy, the one or more access network forwarding settings including one or more restriction settings on the access network forwarding service, at least one of the access network forwarding settings identifying which access network route or traffic redirection is to be used by the first end point device when attempting to forward traffic between the one or more additional end point devices and the access network; and”

The *Thomas-Buddhikot* combination discloses 24[b][i]. EX1003, ¶80.

Thomas’s server provides the hotspot device with a service level. *Supra* § VI.A.2.j.

Thomas’s server 108 modified with *Buddhikot*’s teachings would provide the

Thomas-Buddhikot hotspot device with firewalling and packet-mangling rules.

EX1003, ¶80.

Buddhikot's firewalling and packet-mangling rules are access network forwarding settings included in a service profile because processor 306 (e.g., "service processor") of the *Thomas-Buddhikot* hotspot device forwards data based on these settings. As explained, a POSITA would have found it obvious to modify *Thomas*'s server to provide the firewalling and packet-mangling rules, as taught by *Buddhikot*, to *Thomas*'s hot-spot device. *Supra* §VI.A.1. As discussed, *Buddhikot*'s firewalling rules implemented in the *Thomas-Buddhikot* hotspot device would protect both the *Thomas-Buddhikot* hotspot device and client devices connected to the *Thomas-Buddhikot* hotspot device against traffic coming from malicious sources. EX1016, ¶75; *supra* §VI.A.2.d. Thus, a POSITA would have understood that the firewalling rules constitute restriction settings because they would prevent traffic flow through the *Thomas-Buddhikot* hotspot device when the rules detect that the traffic flow originates from malicious sources. EX1003, ¶81. As also discussed, *Buddhikot*'s packet-mangling rules implemented in the *Thomas-Buddhikot* hotspot device would determine which access network route (e.g., when forwarding traffic to a web server) or redirection (e.g., when forwarding traffic to a local cache) is to be used by the *Thomas-Buddhikot* hotspot device when

attempting to forward traffic between client devices connected to the *Thomas-Buddhikot* hotspot device and the cellular network 102. *Supra* §VI.A.2.d.

m. 24[b][ii]: “transmit the one or more access network forwarding settings to at least one selected from the group consisting of the *first end point device* and at least one of the one or more network elements.”

The *Thomas-Buddhikot* combination discloses 24[b][ii]. EX1003, ¶82. As discussed, the *Thomas-Buddhikot* server would provide (or “transmit”) *Buddhikot*’s firewall and packet-mangling rules to the *Thomas-Buddhikot hotspot device*. *Supra* §VI.A.2.j.

3. Claim 25: “The network system of claim 24, wherein the one or more messages includes credentials specific to the *first end point device*, and wherein the activation sequence is specific to the credentials.”

Thomas discloses claim 25. EX1003, ¶83. *Thomas* discloses a start message sent from *wireless device 110* to server 108. EX1005, ¶58. The start message “includes parameters, such as message type, phone international mobile equipment identification (IMEI), cell identifier, software version, and comments.” EX1005, ¶58. The one or more device parameters are credentials specific to *Thomas*’s *wireless device 110* (e.g., “first end point device”). EX1003, ¶83; EX1001, 135:27-35 (“one or more device parameters (e.g., service owner, device type, OEM, plan type, IP address, security credential and/or software version) are used to determine what the appropriate network provisioning steps and/or settings.”).

Thomas further discloses that server 108 determines, in response to the start message, whether wireless device 110 is authorized to operate within *Thomas*'s network. EX1005, ¶59. According to *Thomas*, “[i]n response to determining whether the wireless device 110 is authorized, the server 108 sends a start response message . . . to the requesting wireless device 110.” EX1005, ¶59. Because the server determines whether the specific end point device is authorized to operate within the network based on the start message, which includes device parameters (e.g., “credentials”), the activation sequence is specific to that device’s credentials. EX1003, ¶84.

4. Claim 26: “The network system of claim 24, wherein a first activation server is configured to re-route the first end point device to a second activation server based on a credential received from the first end point device or based on a query-response sequence.”

Thomas discloses claim 26. EX1003, ¶85. *Thomas* discloses an “add client message” containing “add client message parameters” that include “identification information associated with a billing account for the client computing device 114 [that] may be sent to the server 108 to allow billing for data services.” EX1005, ¶62. Parameters such as identification information associated with a billing account constitute a credential as claimed. EX1003, ¶85; EX1001, 144:61-145:15 (service account “associated with some portion of the credentials”).

According to *Thomas* “the tasks associated with the server 108 may be divided between two servers.” For example, *Thomas* discloses an “authorization server 1202” and a “billing server 1204 connected to the network infrastructure [that] may interact with the authentication server 1202.” EX1005, ¶86. *Thomas* further discloses that “one or more metrics characterizing the connection session may be communicated to the billing server 1204 as the billing server 1204 has a billing relationship with the user of the client computing device 114.” EX1005, ¶87. Communicating metrics regarding a connection session from an authorization server (e.g., “a first activation server”) to a billing server (e.g., “a second activation server”) constitutes re-routing *Thomas*’s hotspot device to a second activation server based on a credential. EX1003, ¶86.

5. Claim 27: “The network system of claim 24, wherein the one or more **activation servers are further configured to provision the **first end point device** by transmitting software for updating the service processor of the **first end point device**.”**

Thomas discloses claim 27. EX1003, ¶87. *Thomas* discloses that a “client access application 312 can provide application-level point of presence capabilities within the **wireless device 110**.” EX1005, ¶34. According to *Thomas*, “[s]cheduled upgrades for the current version of the client access applications 312 running throughout the network and for the server access applications 406 may be scheduled and performed” by **server 108**. EX1005, ¶41. Thus, **server 108** in

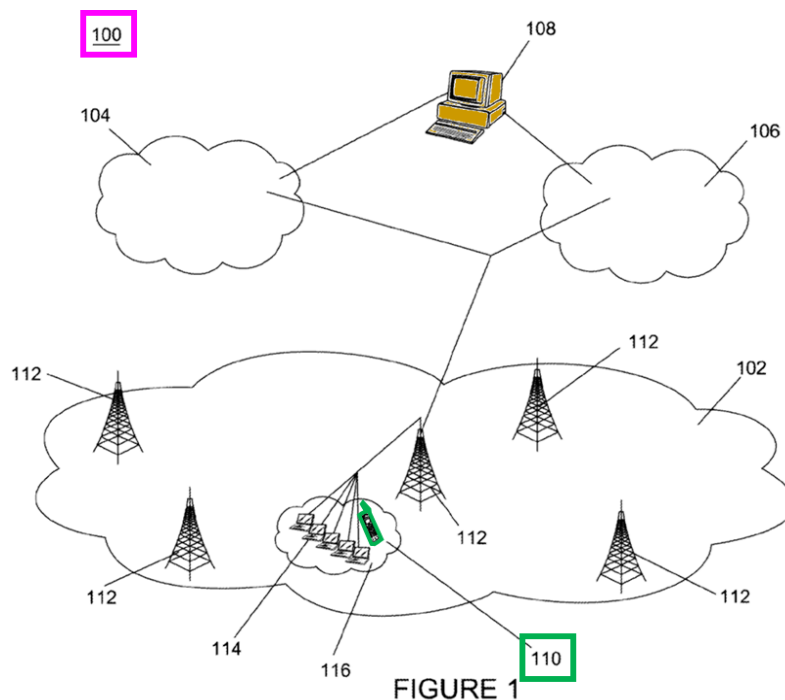
Thomas's network system 100 can provision wireless device 110 by upgrading the client access application. EX1003, ¶87.

6. Claim 28: “The network system of claim 24, wherein the one or more activation servers are operated by a virtual service provider, and wherein the virtual service provider bills a user of the first end point device for the access network forwarding service and provides a payment to a provider of the access network.”

Thomas discloses claim 28. EX1003, ¶¶88. *Thomas* discloses that the forwarding service may be hosted by a mobile virtual network operator (“MVNO”), “which is a company that does not own any licensed frequency spectrum, but resells wireless services under their own brand name, using the network of another mobile phone operator.” EX1005, ¶¶81, 94. According to *Thomas*, the MVNO (e.g. “virtual service provider”) may provide server 108. EX1003, ¶88. *Thomas* further discloses that “[b]illing measures are established for use of the network infrastructure by a computing device.” EX1005, ¶79. Because the MVNO of *Thomas* resells wireless services, it would bill a user of the *Thomas-Buddhikot* hotspot device for the access network forwarding service and provide a payment to a provider of the access network. EX1003, ¶88.

7. **Claim 29:** “The network system of claim 24, wherein the one or more network elements include at least one of **an authentication and authorization server**, a billing system, and one or more gateways.”

Thomas discloses claim 29. EX1003, ¶89. As discussed for element 24[a], *Thomas*’s network system 100 includes at least one **server 108**. *Supra* § VI.A.2.g; EX1005, Fig. 1.



EX1005, Fig. 1 (annotated). *Thomas* discloses that “the tasks associated with the server 108 may be divided between two servers.” For example, *Thomas* discloses that an “**authorization server 1202** provides authorization for communication to the network infrastructure . . . [and a] billing server 1204 connected to the network infrastructure may interact with the **authentication server 1202**.” EX1005, ¶86.

Thus, *Thomas* discloses at least an authentication and authorization server 1202.

EX1003, ¶89.

8. Claim 30: “The network system of claim 29, wherein the service controller is further configured to assign the data to one or more specific access network routing paths.”

Thomas discloses claim 30. EX1003, ¶90. *Thomas* discloses that a firewall and virtual private network may operate on wireless device 110 or server 108. EX1005, ¶42. As explained for claim 24[pre][iii], the firewall service on the *Thomas-Buddhikot* hotspot device blocks transfer of packets to prevent malicious attacks on the clients and allows packets to be transferred between WWAN and WLAN based on firewall rules. *Supra* §VI.A.2.d. Because *Thomas*’s firewall can operate on server 108, in some embodiments, processor 402 of server 108 (e.g., “service controller”) would be configured to block the transfer of packets to prevent malicious attacks on the clients and allow packets to be transferred between WWAN and WLAN based on firewalling and packet-mangling rules (e.g., “assign the data to one or more specific access network routing paths”). A POSITA would understand processor 306 of *Thomas*’s hotspot device to do the same. EX1003, ¶90; *supra* §VI.A.2.d.

9. Claim 31: “The network system of claim 24, wherein at least one of the one or more access network forwarding settings configures the forwarding agent to begin providing the forwarding of the data.”

The *Thomas-Buddhikot* combination discloses claim 31. EX1003, ¶91. As explained in element 24[b][i], *Buddhikot*’s firewalling and packet-mangling rules are access network forwarding settings as claimed. *Supra* §VI.A.2.1. As explained in element 24[pre][iii], *Thomas*’s **software** configured to forward data (e.g., “policy implementation agent”) between the **radio frequency front end** and the **wireless network radio front end**, and a **firewall** (e.g., “firewall agent”) of *Thomas*’s hotspot device constitutes the claimed forwarding agent. *Supra* §VI.A.2.d. As also explained in element 24[pre][iii], in the *Thomas-Buddhikot* hotspot device, the firewall service is configured to forward or redirect data based on packet-mangling rules. *Supra* §VI.A.2.d; EX1003, ¶91.

10. Claim 32: “The network system of claim 24, wherein at least one of the one or more access network forwarding settings is a function of a network congestion state.”

The *Thomas-Buddhikot* combination discloses claim 32. EX1003, ¶92. As explained in element 24[b][i], the firewalling and packet-mangling rules of *Buddhikot* are the access network forwarding settings included in a service profile because processor 306 (e.g., “service processor”) of the *Thomas-Buddhikot* hotspot device forwards data based on these settings. *Supra* §VI.A.2.1.

Thomas further discloses that usage of the forwarding service can be metered based on “peak or off-peak usage, or elevated quality of service requirements such as may be required for latency sensitive applications.” EX1005, ¶54. Thus, *Thomas* discloses forwarding data through its hotspot device based on quality of service. EX1003, ¶93.

Buddhikot discloses providing “Quality of Service in the form of multiple service classes, each with a guaranteed minimum bandwidth.” EX1016, ¶78. According to *Buddhikot*, if “extra bandwidth is available, users can exceed their minimum rate, with high class users getting the priority to grab excess resources.” EX1016, ¶78 *Buddhikot*’s gateway 40 “control[s] the amount of traffic which competes for resources, instead of prioritizing traffic when congestion occurs.” EX1016, ¶79. For example, “[a]t first, a single user gets 3.5 Mbps . . . [and as] a second and a third user arrives, they all get equal share of the available bandwidth which is around 4.5 Mbps,” such that “each user has the same QoS level.” EX1016, ¶177. Thus, *Buddhikot* discloses data forwarding settings that adjust the available bandwidth based on network congestion. EX1003, ¶94.

As explained, a POSITA would have found it obvious to implement *Buddhikot*’s congestion management scheme as part of the access network forwarding settings implemented on *Thomas*’s hotspot device. *Supra* §VI.A.1.b; EX1003, ¶95.

11. Claim 34: “The network system of claim 24, wherein the one or more restriction settings includes a setting for enabling or disabling the access network forwarding service.”

The *Thomas-Buddhikot* combination discloses claim 34. EX1003, ¶96. As explained element 24[pre][iii], in the *Thomas-Buddhikot* hotspot device, the firewall service is configured to use packet filtering rules to protect the *Thomas-Buddhikot* hotspot device and/or client devices connected to the *Thomas-Buddhikot* hotspot device from malicious attacks. *Supra* §VI.A.2.d. A POSITA would have understood that applying firewall rules would block data flow through the *Thomas-Buddhikot* hotspot device if the data originated from a malicious source. EX1003, ¶96. A POSITA would have further understood that by blocking data flow in this manner, the firewall rules in the *Thomas-Buddhikot* hotspot device would implement a restriction setting that disables the flow of data between client devices connected to the *Thomas-Buddhikot* hotspot device and the cellular network 102, thereby disabling the access network forwarding service. EX1003, ¶96.

12. Claim 36: “The network system of claim 34, wherein a particular restriction setting is on a usage of a forwarding connection of the access network forwarding service, wherein the forwarding connection connects the one or more additional end point devices to the access network via the forwarding agent.”

The *Thomas-Buddhikot* combination discloses claim 36. EX1003, ¶97. *Thomas* discloses that “multiple client computing devices 114 may join during an active session of the client access application 312.” EX1005, ¶64. Thus, *Thomas*

discloses that its hotspot device provides a forwarding connection to allow more than one client devices 114 to exchange data with *Thomas's* cellular network 102. EX1003, ¶97. As explained for claim 32, data is forwarded in the *Thomas-Buddhikot* hotspot device based on QoS rules as taught by *Buddhikot*. *Supra* §VI.A.10; EX1003, ¶97. As also explained, the QoS rules restrict the bandwidth for multiple connected client devices such that all connected client devices may continue to exchange data with the cellular network 102. *Supra* §VI.A.10; EX1003, ¶97. A POSITA would have understood that the QoS rules causing bandwidth restrictions would constitute restriction settings on the usage of the forwarding connection of the *Thomas-Buddhikot* hotspot device. EX1003, ¶97.

13. Claim 40: “The network system of claim 24, wherein the service controller is further configured to provide a forwarding service notification to the first end point device or to an additional end point device during use of the access network forwarding service.”

Thomas discloses claim 40. EX1003, ¶98. *Thomas's* discloses a “user interface screen 900 . . . that provides connection information for the wireless device 110.” EX1005, ¶76, Fig. 9.

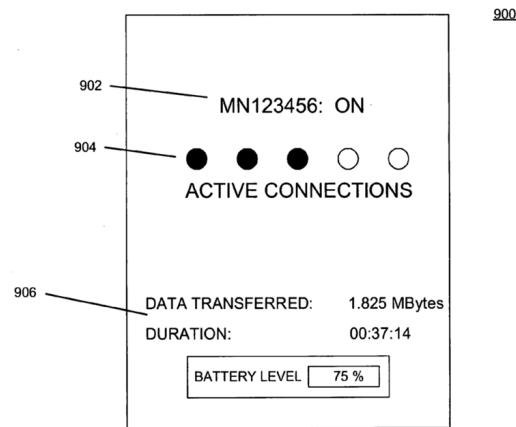


FIGURE 9

EX1005, Fig. 9. *Thomas* further discloses notifications that “provide[] detailed information, such as transferred data quantities, duration of the present session, and battery level.” EX1005, ¶76. *Thomas* discloses notifications that include a “startup ... message display sequence” associated with activating the forwarding service, as the startup messages involve requesting authorization from server 108 to run application 312. EX1005, ¶¶59, 77, Fig. 10. The notifications also include an “activation status” indicating if the forwarding service is on, as well as notifications of authorized devices. EX1003, ¶98.

14. Claim 41: “The network system of claim 40, wherein the forwarding service notification is provided when the access network forwarding service is enabled and the at least one access network includes a roaming access network.”

Thomas discloses claim 41. EX1003, ¶¶99. *Thomas* discloses notifications that include a “startup ... message display sequence” associated with activating the forwarding service, as the startup messages involve requesting authorization from

server 108 to run application 312. EX1005, ¶¶59, 77, Fig. 10. The notifications also include an “activation status” indicating if the forwarding service is on, as well as notifications of authorized devices. EX1003, ¶99. Accordingly, *Thomas* discloses providing the forwarding service notification when the access network forwarding service is enabled.

Thomas also discloses that a “roaming management function may be performed to run on top of the WAN transport supplied by a given carrier.” EX1005, ¶71. *Thomas* states that “data plans may be provided by which a user may include roaming within the plan coverage.” EX1005, ¶71. Thus, *Thomas* discloses that connection of *Thomas*’s hotspot device to the cellular network 102 may be a roaming connection. EX1003, ¶100. A POSITA would have understood that the forwarding service notification disclosed by *Thomas* is provided when the access network is a roaming access network. EX1003, ¶100.

15. Claim 42: “The network system of claim 40, wherein the forwarding service notification informs the user of **an amount of usage of the access network forwarding service, a rate of usage of the access network forwarding service, that the access network forwarding service is being used on a particular access network, that a service usage restriction setting is in place for the access network forwarding service, that the access network forwarding service is available or that the access network forwarding service is not available.”**

Thomas discloses claim 42, where the term “or” requires only one of the listed features to satisfy the claim. EX1003, ¶101. *Thomas* discloses a user

interface that provides “detailed information, such as transferred data quantities, duration of the present session, and battery level.” EX1005, ¶76, Fig. 9. Thus, *Thomas*’s user interface displays a notification about the amount of usage of the access network forwarding service. EX1005, ¶76, Fig. 9.

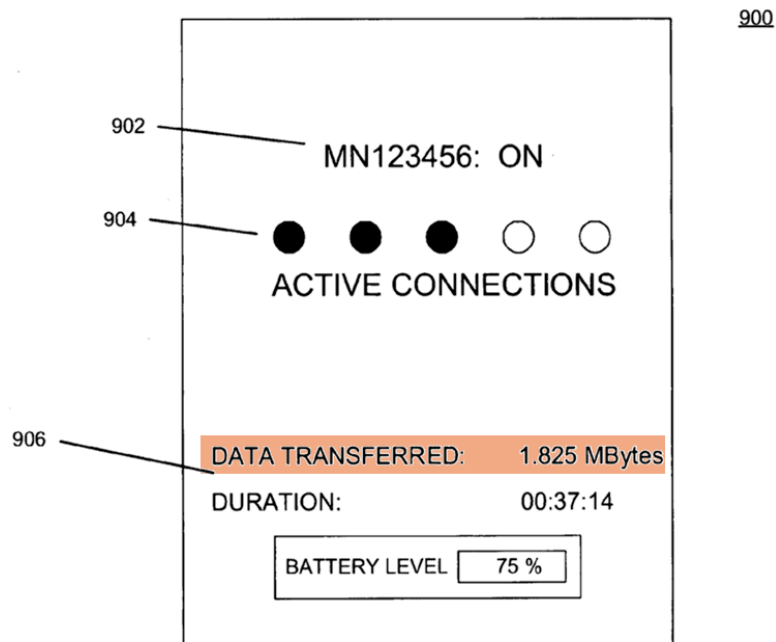


FIGURE 9

EX1005, Fig. 9 (annotated).

16. Independent Claim 44

a. 44[pre]: “A method comprising:”

Thomas discloses 44[pre]. EX1003, ¶102. *Thomas*’s Figure 11 illustrates an exemplary process for providing mobile network access. EX1005, ¶¶21, 79. As explained below, the *Thomas-Buddhikot* network environment, including the *Thomas-Buddhikot* hotspot device performs all the method steps.

b. 44[a][i]: “receiving, at a **service design system**, first service plan elements of a first service plan for using **an access network forwarding service**, the access network forwarding service to be used by **a first end point device**,”

The *Thomas-Buddhikot* combination discloses 44[a][i], as discussed below.

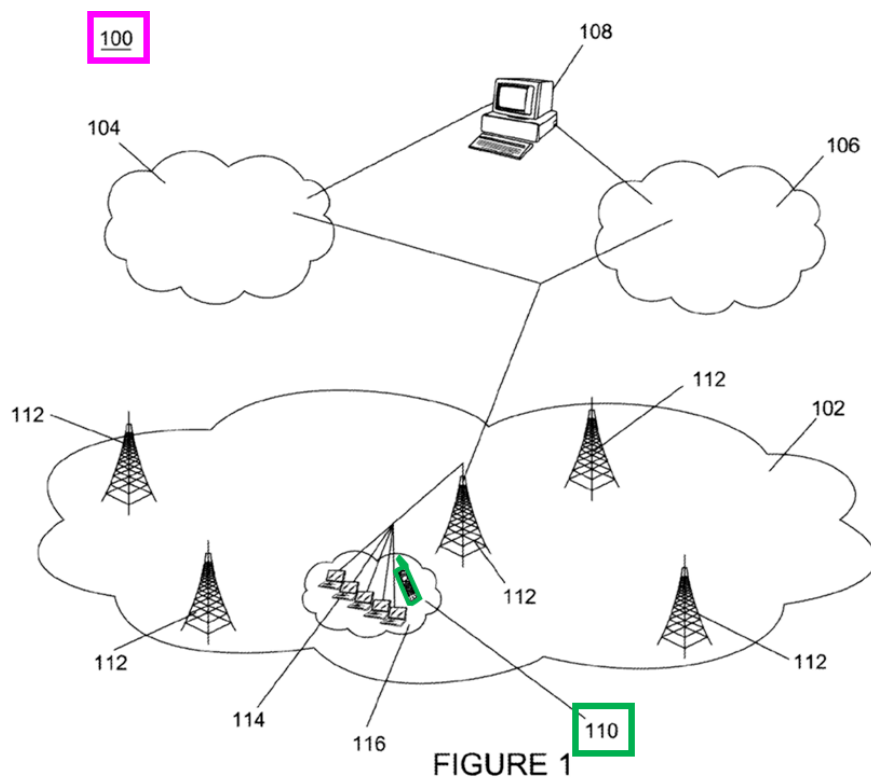
Infra §VI.A.16.c; EX1003, ¶103.

c. 44[b][i] “wherein the first service plan elements include one or more access network forwarding settings that define one or more restriction settings on the access network forwarding service, the one or more access network forwarding settings identifying which access network route or traffic redirection is to be used by the first end point device when attempting to forward traffic between the one or more additional end point devices and the access network;”

The *Thomas-Buddhikot* combination discloses 44[a][i] and 44[b][i].

EX1003, ¶104. *Thomas* discloses a **network environment 100**. EX1005, ¶24, Fig.

1. A POSITA would have understood that *Thomas*’s **network environment 100** as modified by *Buddhikot* is a service design system as claimed. EX1003, ¶104. As explained for element 24[pre], *Thomas*’s **network environment 100** includes **wireless device 110** (e.g., “first end point device”) capable of **providing data services to client computing devices 114** by **communicating normal traffic through the wireless device 110 to reach a network** (e.g., “using an access network forwarding service”). EX1005, ¶¶25, 47, Fig. 1; *supra* §VI.A.2.a.



EX1005, Fig. 1.

The table below compares limitation 44[b][i] with 24[b][i] with corresponding recitations in bold font.

Claim 44[b][i]	Claim 24[b][i]
wherein the first service plan elements include one or more access network forwarding settings that define one or more restriction settings on the access network forwarding service, the one or more access network forwarding settings identifying which access network route or traffic redirection is to be used by the first end point device when attempting to forward traffic between the one or more additional end point devices and the access network	obtain a service profile including one or more access network forwarding settings for the access network forwarding policy, the one or more access network forwarding settings including one or more restriction settings on the access network forwarding service, at least one of the access network forwarding settings identifying which access network route or traffic redirection is to be used by the first end point device when attempting to forward traffic between the one or more additional end point devices and the access network

Accordingly, the service plan elements of claim 44[b][i] correspond to access network forwarding settings of the service profile of claim 24[b][i].

EX1003, ¶¶105-06. As explained for element 24[b][i], the *Thomas-Buddhikot* hotspot device receives access network forwarding settings, including, QoS, firewall, and packet-mangling rules from the *Thomas-Buddhikot* server. *Supra* §VI.A.2.1. As also explained, the firewalling and packet-mangling settings provide the claimed restriction settings. *Supra* §§VI.A.2.d, VI.A.2.1. As also explained, a POSITA would have been motivated to implement *Buddhikot*'s QoS, firewall, and packet-mangling rules in *Thomas*'s hotspot device with a reasonable expectation of success. *Supra* §VI.A.1.a. Thus, for the same reasons discussed above for claim

24[b][i], the *Thomas-Buddhikot* combination renders obvious elements 44[a][i] and 44[b][i]. EX1003, ¶¶106-09.

d. **44[a][ii]: “the first end point device including an access network modem configured to communicate data over at least one access network, the access network modem providing a connection via at least one 2G, 3G or 4G wireless network, and”**

Thomas discloses 44[a][ii] for the same reasons discussed above for 24[pre][i]. *Supra* §VI.A.2.b; EX1003, ¶¶110-11.

e. **44[a][iii]: “a local area network modem configured to communicate data with one or more additional end point devices over a local area network, the local area network modem providing a connection via at least one of Bluetooth, Wi-Fi or USB;”**

Thomas discloses 44[a][iii] for the same reasons discussed above for 24[pre][ii]. *Supra* §VI.A.2.c; EX1003, ¶¶112-13.

f. **44[b]: “generating an access network forwarding policy based on the first service plan elements, the access network forwarding policy defining a state of a forwarding connection, wherein the forwarding connection is configured to communicate the data between the one or more additional end point devices and the access network via the local area network modem and the access network modem,”**

The *Thomas-Buddhikot* combination discloses 44[b]. EX1003, ¶114. As discussed in 24[b][i], the *Thomas-Buddhikot* hotspot device receives access

network forwarding settings, including QoS, firewall, and packet-mangling rules from the *Thomas-Buddhikot* server. *Supra* §VI.A.2.1; EX1003, ¶114.

Thomas discloses that in “response to receipt of the start message, the server 108 determines whether the requesting wireless device 110 is authorized to operate within the network.” EX1005, ¶59. *Thomas* also discloses that upon determining that the wireless device 110 is authorized, “server 108 sends a start response message,” including parameters such as a response (e.g., okay to run or never start) and service level to the requesting wireless device 110. EX1005, ¶59. Thus, *Thomas*’s server 108 modified to include *Buddhikot*’s QoS, firewalling, and packet-mangling rules in the service level would generate the start message containing these access network forwarding settings. EX1003, ¶115. By generating the start message containing the access network forwarding settings, the *Thomas-Buddhikot* server generates the access network forwarding policy based on the first service plan elements (e.g., the access network forwarding settings).

The access network forwarding settings sent to the *Thomas-Buddhikot* hotspot device also include the “response (e.g., okay to run or never start).” EX1005, ¶59. Thus, the access network forwarding policy based on the first service plan elements defines the state (e.g., run or not run) of the *Thomas-Buddhikot* hotspot device. EX1003, ¶116.

As discussed for element 24[pre][iii], the *Thomas-Buddhikot* hotspot device provides a forwarding connection or forwarding service that allows data to flow between its **radio frequency front end 300** (e.g., “access network modem”) and its **wireless network radio front end** (e.g., “local area network modem”). *Supra* §VI.A.2.d. Thus, determining a state (e.g., run or not run) of the *Thomas-Buddhikot* hotspot device also determines the state—active or inactive—of the forwarding connection provided by the *Thomas-Buddhikot* hotspot device. EX1003, ¶117.

g. 44[c]: “associating the first end point device with the first service plan;”

The *Thomas-Buddhikot* combination discloses 44[c]. EX1003, ¶118. *Thomas* discloses that in response to receiving a start message, the wireless device 110 either starts the client access application 312 or stops its attempts, depending upon whether the parameter sent indicates that it is okay to run the client access application or whether it should never start. EX1005, ¶60. *Thomas* also discloses that wireless device 110 receives a service level in the start response message. EX1005, ¶59. As explained, the service level includes one or more settings or rules for forwarding data through wireless device 110. *Supra* §VI.A.2.d.

Buddhikot discloses agents in a gateway device that install firewalling and packet-mangling rules. EX1016, ¶75. As explained, a POSITA would have been

motivated to install *Buddhikot*'s firewalling and packet-mangling rules on *Thomas*'s hotspot device. *Supra* §VI.A.1.a. A POSITA would have also understood that by starting the client access application 312 and by installing the firewalling and packet-mangling rules, the *Thomas-Buddhikot* hotspot device is associated with the first service plan that includes the firewalling and packet-mangling rules. EX1003, ¶119.

h. 44[d]: “translating the access network forwarding policy to first instructions; and,”

The *Thomas-Buddhikot* combination discloses 44[d]. EX1003, ¶120. *Thomas* discloses that “software running on the wireless device 110 enables the distribution of the data services offered by the cellular network 102 to be distributed in local area networks (LAN) or small area networks supported by 802.11 and analogous WLAN technologies supported on the wireless device 110.” EX1005, ¶¶30, 46. Both *Thomas* and *Buddhikot* disclose programming the rules and the use of software to control the flow of data through the *Thomas-Buddhikot* hotspot device. EX1003, ¶120. As explained, a POSITA would have been motivated to cause installation of *Buddhikot*'s firewalling and packet-mangling rules on *Thomas*'s hotspot device. *Supra* §VI.A.1.a. A POSITA would have understood that programming software and/or installing rules requires translating the rules in the access network forwarding policy into program instructions that

can be executed by a processor of the *Thomas-Buddhikot* hotspot device. EX1003, ¶120.

- i. **44[e]: “providing the first instructions to one or more policy implementation agents, the one or more policy implementation agents capable of implementing the access network forwarding policy for the first end point device.”**

Thomas discloses 44[e]. EX1003, ¶121. *Thomas* discloses that “software running on the wireless device 110 enables forwarding of data between client devices connected to wireless device 110 via WLAN technologies and cellular network 102.” EX1005, ¶¶30, 46. *Thomas* explains that “wireless device 110 route[s] the packets for communication sessions between a laptop and the Internet 104.” EX1005, ¶50. As explained in 24[pre][iii], **software** configured to forward data between a **radio frequency front end** and a **wireless network radio front end** of *Thomas*’s hotspot device constitutes one or more **policy implementation agents**. *Supra* §VI.A.2.d. As also explained, the policy implementation agent in the *Thomas-Buddhikot* hotspot device forwards data based on parameters such as metered usage, quality of service requirements, firewalling and packet-mangling rules, and other factors, included in the access network forwarding policy. *Supra* §VI.A.2.d; EX1003, ¶¶121-23.

17. Claim 49: “The method of claim 44, wherein a particular restriction setting is on a usage of a forwarding connection of the access network forwarding service, wherein the forwarding connection connects the one or more additional end point devices to the access network via the forwarding agent.”

The *Thomas-Buddhikot* combination discloses claim 49 for the same reasons as claim 36. *Supra* §VI.A.12; EX1003, ¶124.

18. Claim 50: “The method of claim 44, wherein the one or more policy implementation agents include the first end point device.”

Thomas discloses claim 50. EX1003, ¶125. As explained above in [44]e, the *Thomas-Buddhikot* hotspot device forwards traffic between client computing devices 114 and the internet according to the access network forwarding policy, making the *Thomas-Buddhikot* hotspot device, including its software, a policy implementation agent. *Supra* §VI.A.16.i; EX1003, ¶125.

B. Ground 2: Claim 33 Is Obvious over *Thomas*, *Buddhikot*, and *Haller*

1. Claim 33: “The network system of claim 24, wherein at least one of the one or more access network forwarding settings is a function of a time of day.”

Claim 33 depends from claim 24, which would have been obvious as discussed above. *Supra* §VI.A.2; EX1003, ¶126. The *Thomas-Buddhikot-Haller* combination discloses the additional features of claim 33. *Haller* discloses that its cellular phone hotspot device includes service level verification software that enforces service level agreements with users. EX1013, ¶¶54-56, 61, 140. *Haller*

also discloses that a user may “generate an unlimited amount of cellular traffic from device 106 during the night but a limited amount during the day.” EX1013, ¶141. *Haller* explains that “during the day, if the limited amount [of cellular traffic] is exceeded no more traffic can be generated from device 106 and packets are dropped” by the service level verification software. EX1013, ¶141. The *Thomas-Buddhikot* hotspot device as modified by *Haller* would include access network forwarding settings to restrict the amount of data being forwarded by the *Thomas-Buddhikot* hotspot device based on a time of day. EX1003, ¶125.

A POSITA would have been motivated to combine the access network forwarding setting restrictions based on the time of day, as disclosed by *Haller*, with the *Thomas-Buddhikot* hotspot device with a reasonable expectation of success. Like *Thomas* and *Buddhikot*, *Haller* is also analogous art to the ’425 patent. It is in the same field of endeavor: mobile devices and wireless access points for computer networking. EX1013, Abstract, ¶¶7, 15, 35-37, 54, 56, Figs. 1-6. Like *Thomas* and *Buddhikot*, *Haller* also shares a common goal with the ’425 patent: using end-user devices for bridging or routing traffic from other devices to a network system (e.g., the internet), including the provisioning of services seeking to improve the customizability and monetization of mobile-hotspot technology (e.g., usage control, user interactivity and notifications via graphical user

interfaces, and billing features). EX1013, Abstract, ¶¶7, 15, 35-37, 54, 56, 90-91, 104, 121-124, 129, 139-141, Figs. 1-6; EX1003, ¶127.

Haller discloses limiting traffic during the day because many users desire to access the network. EX1013, ¶141; EX1003, ¶128. At night, the demand is lower, which allows use of an unlimited amount of cellular traffic. EX1013, ¶141; EX1003, ¶128. The *Thomas-Buddhikot* network system implements forwarding settings based on bandwidth. *Supra* §§VI.A.2.d, VI.A.2.i. A POSITA would have been motivated to implement *Haller*'s time-of-day-based traffic control in the *Thomas-Buddhikot* network system to obtain the benefits of allowing a maximum number of users to access the network via the *Thomas-Buddhikot* hotspot device when demand is high. EX1003, ¶128. Doing so would minimize the number of users that are denied access to the access network, thereby improving overall user experience and reducing overall user dissatisfaction. EX1003, ¶128.

The combination of *Haller*'s bandwidth rules with the *Thomas-Buddhikot* network system would have been a combination of familiar elements (e.g., bandwidth control rules) according to known methods (e.g., implementing the bandwidth control rules in a manner similar to implementation of the firewall and packet-mangling rules) to obtain predictable results (e.g., maximizing the number of connected users). EX1003, ¶129; *KSR*, 550 U.S. at 416. A POSITA would have

had a reasonable expectation of success in implementing *Haller*'s bandwidth control rules on the *Thomas-Buddhikot* hotspot device. EX1003, ¶129.

As explained, implementing rules on *Thomas*'s hotspot device would have involved known techniques as disclosed by *Thomas* and *Buddhikot* and would have been well within the skill level of a POSITA. *Supra* §VI.A.1; EX1003, ¶130. Accordingly, a POSITA would have had a reasonable expectation of success in combining *Haller*'s teachings with the *Thomas-Buddhikot* network system. EX1003, ¶130.

C. Ground 3: Claims 39, 43, and 45 Are Obvious over *Thomas, Buddhikot, and Polson*

1. Motivation to combine *Thomas, Buddhikot, and Polson*

Like *Thomas* and *Buddhikot*, *Polson* is also analogous art to the '425 patent. EX1003, ¶131. It is in the same field of endeavor: mobile devices and wireless access points for computer networking. EX1015, Abstract, ¶¶2, 16, 20-23, 26, 56, Figs. 1, 2, 9-15. Like *Thomas* and *Buddhikot*, *Polson* also shares a common goal with the '425 patent: using end-user devices for bridging or routing traffic from other devices to a network system (e.g., the internet), including the provisioning of services seeking to improve the customizability and monetization of mobile-hotspot technology (e.g., usage control, user interactivity and notifications via

graphical user interfaces, and billing features). EX1015, Abstract, ¶¶2, 16, 20-23, 26, 29-35, 38-39, 44-46, 52-53, 56, 78-79, Figs. 1, 2, 9-15; EX1003, ¶131.

a. Different settings for different access networks

Polson discloses a hotspot device that can connect to multiple WWANs. EX1015, ¶¶20, 52-55. *Polson* explains that doing so “facilitates the switching of WWAN interfaces in areas where another provider having a different WWAN interface is stronger, or where the provider associated with the current WWAN interface 110 does not provide service.” EX1015, ¶¶52-55. This “facilitates the mobility of the gateway 108.” EX1015, ¶53; EX1003, ¶132.

A POSITA would have been motivated to implement the multiple WWAN capability of *Polson* on the *Thomas-Buddhikot* hotspot device. EX1003, ¶133. Doing so would have enabled the *Thomas-Buddhikot* hotspot device to allow client devices to exchange data with the internet in different geographic locations even if one or more cellular networks did not provide service in that geographical location. A POSITA would have been motivated to operate the *Thomas-Buddhikot* hotspot device based on the service agreements (e.g., access network forwarding settings) associated with a particular WWAN modem to ensure the cellular networks are able to accurately bill the clients for their usage of the respective WWANs. EX1003, ¶133.

Implementing *Polson*'s teaching of connecting to multiple cellular networks on the *Thomas-Buddhikot* hotspot device would have been a combination of familiar elements (WWAN modems capable of exchanging data with different cellular networks) according to known methods (e.g., providing more than one WWAN modem in the *Thomas-Buddhikot* hotspot device) to obtain predictable results (e.g., ensuring client devices connected to the *Thomas-Buddhikot* hotspot device can exchange data with the internet in different geographical locations). EX1003, ¶134; *KSR*, 550 U.S. at 416. A POSITA would have had a reasonable expectation of success in implementing *Polson*'s multiple WWAN capability on the *Thomas-Buddhikot* hotspot device. EX1003, ¶134. *Thomas* already discloses a hotspot device having a WWAN modem. *Supra* §§VI.A.2.b, VI.A.2.c. *Polson* discloses that its gateway includes devices like *Thomas*'s hotspot device, capable of facilitating transmission of data between LANs and WANs. EX1015, ¶20. *Polson* also discloses a gateway device that has more than one WWAN modem. EX1015, ¶¶52-55. Thus, implementing more than one WWAN modem on the *Thomas-Buddhikot* hotspot device would have involved known techniques as disclosed by *Polson* and would have been well within the skill level of a POSITA. EX1003, ¶134. Accordingly, a POSITA would have had a reasonable expectation of success in combining *Polson*'s teachings with *Thomas* and *Buddhikot*. EX1003, ¶134.

b. Restriction to a maximum number of additional end point devices.

As discussed, *Thomas*, *Buddhikot*, and *Polson* are analogous art to the '425 patent. *Supra* §VI.C.1.a. *Polson* also discloses establishing “limitations on the number of simultaneous WiFi . . . connections.” EX1015, ¶30. A POSITA would have understood that such limitations may ensure that each device connected via the WiFi connection can access the network using a minimum bandwidth to ensure user satisfaction with the connection. EX1003, ¶135.

A POSITA would have been motivated to implement the limitation on the number of simultaneous WiFi connections as taught by *Polson* on the *Thomas-Buddhikot* hotspot device to obtain the same benefits—namely, adequate minimum bandwidth for each WiFi connection. EX1003, ¶136. For example, *Thomas* already discloses a maximum number of available IP addresses for the WLAN connections. EX1005, ¶69. Implementing *Polson*’s limits would constitute a combination of familiar elements (e.g., a setting specifying maximum number of simultaneous WiFi connections) according to known methods (e.g., implementing rules in the *Thomas-Buddhikot* hotspot device) to obtain predictable results (e.g., ensuring client devices connected to the *Thomas-Buddhikot* hotspot device can exchange data with the internet at a minimum bandwidth). EX1003, ¶136; *KSR*, 550 U.S. at 416.

A POSITA would have had a reasonable expectation of success in implementing *Polson*'s limits on the maximum number of simultaneous WiFi connections on the *Thomas-Buddhikot* hotspot device. EX1003, ¶137. *Thomas* already discloses rules that specify the maximum number of available IP addresses. EX1005, ¶69. The *Thomas-Buddhikot* combination also already discloses techniques for implementing additional firewalling and packet-mangling rules on the *Thomas-Buddhikot* hotspot device. *Supra* §VI.A.1.a. Thus, implementing *Polson*'s restriction setting or rule limiting the maximum number of simultaneous WiFi connections on the *Thomas-Buddhikot* hotspot device would have involved known techniques as disclosed by *Thomas*, *Buddhikot*, and *Polson* and would have been well within the skill level of a POSITA. EX1003, ¶137. Accordingly, a POSITA would have had a reasonable expectation of success in combining *Polson*'s teachings with *Thomas* and *Buddhikot*. EX1003, ¶137.

2. Claim 39: “The network system of claim 24, wherein the one or more access network forwarding settings includes at least one setting that is different for different access networks, each providing an access network forwarding service.”

Claim 39 depends from claim 24, which would have been obvious as discussed above. *Supra* §VI.A.2; EX1003, ¶138. The *Thomas-Buddhikot-Polson* combination discloses the additional features of claim 39. As explained, the *Thomas-Buddhikot* hotspot device provides access network forwarding services

based on one or more forwarding settings. *Supra* §§VI.A.2.d, VI.A.2.1. *Polson* discloses a gateway that connects devices to a 3G cellular-access network. EX1015, Abstract, ¶¶16, 20-23, 26, 29-33. *Polson* discloses that “more than one WWAN interface 110 may be available for use by gateway 108 to establish a WWAN 112 connection” and that the gateway may operate each interface according to an associated service agreement. EX1015, ¶29. *Polson* discloses that the service agreements may restrict access in many ways, including QoS (e.g., sufficient bandwidth to support Voice-over-IP), throughput provided, or cumulative bits over time. EX1015, ¶30. *Polson* also discloses that its gateway facilitates switching of WWAN interfaces in areas where another provider having a different WWAN interface is stronger, or where the provider associated with the current WWAN interface 110 does not provide service. EX1015, ¶52; EX1003, ¶138.

As discussed, a POSITA would have found it obvious to combine *Polson*’s multiple WWAN capability with the *Thomas-Buddhikot* hotspot device to be able to use the *Thomas-Buddhikot* hotspot device with different cellular networks in different geographies. *Supra* §VI.C.1. A POSITA would have also found that at least one access network forwarding setting (e.g., throughput or cumulative number of bits) would be different for the different access networks based on the

service agreement associated with the cellular network being used by the *Thomas-Buddhikot-Polson* hotspot device. EX1003, ¶139.

3. Claims 43 and 45:

a. 43: “The network system of claim 24, wherein a particular restriction setting restricts a forwarding connection of the network access forwarding service to a maximum number of additional end point devices, wherein the forwarding connection connects the one or more additional end point devices to the access network via the forwarding agent.”

Claim 43 depends from claim 24, which would have been obvious as discussed above. *Supra* §VI.A.2; EX1003, ¶140. The *Thomas-Buddhikot* combination alone or with *Polson* discloses the additional features of claim 43. As explained, the *Thomas-Buddhikot* combination discloses a network system wherein the forwarding connection connects the one or more additional end point devices to the access network via the forwarding agent. *Supra* §VI.A.12. As also explained, the *Thomas-Buddhikot* combination discloses restriction settings for the forwarding connection. *Supra* §§VI.A.2.1, VI.A.17.c; EX1003, ¶140.

Thomas discloses restriction settings that specify a maximum number of end point devices. EX1005, ¶¶59, 69. For example, *Thomas* discloses that the start response message sent by its server 108 to wireless device 110 includes parameters such as a “number of available IP addresses.” EX1005, ¶¶59, 69. A POSITA would have understood that the *Thomas-Buddhikot* hotspot device would not be able to

connect additional client devices if the total number of connected devices exceeded the maximum number of available IP addresses. EX1003, ¶141. Thus, the *Thomas-Buddhikot* combination alone discloses the additional limitations of claim 43.

To the extent Patent Owner disputes that the *Thomas-Buddhikot* combination discloses the additional features of claim 43, *Polson* discloses these limitations. *Polson* discloses that “the gateway may inquire of a server, such as a server associated with the gateway or with a wireless service provider, as to the existence and features of a service agreement associated with one of a number of inputs. ... Exemplary features include a limitation on a number of simultaneous WiFi or Ethernet LAN connections of the gateway.” EX1015, ¶78. As discussed, a POSITA would have found it obvious to combine *Polson*’s limitation on a number of simultaneous WiFi or Ethernet LAN connections of the gateway with the *Thomas-Buddhikot* hotspot device. *Supra* §VI.C.1; EX1003, ¶142.

b. 45: “The method of claim 44, wherein a particular restriction setting restricts use of the forwarding connection of the network access forwarding service to a maximum number of additional end point devices.”

Claim 45 depends from claim 44, which would have been obvious as discussed above. *Supra* §VI.A.16; EX1003, ¶143. The *Thomas-Buddhikot* combination alone or with *Polson* discloses the additional features of claim 45 for

the same reasons discussed above for claim 43. *Supra* §VI.C.3.a; EX1003, ¶143-46.

D. Ground 4: Claims 35, 37, 38, 46, 47, and 48 Are Obvious over *Thomas*, *Buddhikot*, and *Weintraub*

1. Motivation to combine *Thomas*, *Buddhikot*, and *Weintraub*

Like *Thomas* and *Buddhikot*, *Weintraub* is also analogous art to the '425 patent. EX1003, ¶147. It is in the same field of endeavor: mobile devices and wireless access points for computer networking. EX1017, Abstract, ¶¶10-15, 19, 21, Figs. 1-8. Like *Thomas* and *Buddhikot*, *Weintraub* also shares a common goal with the '425 patent: using end-user devices for bridging or routing traffic from other devices to a network system (e.g., the internet), including the provisioning of services seeking to improve the customizability of mobile-hotspot technology (e.g., usage control, user interactivity and notifications via graphical user interfaces). EX1017, Abstract, ¶¶10-15, 19, 21, 25-27, 31-32, Figs. 1-8. EX1003, ¶147.

a. Network traffic classification of the data

Weintraub discloses a variety of network traffic classifications such as VOIP, IM, e-mail, and other types of traffic. EX1017, ¶¶25-26; EX1003, ¶148. *Weintraub* also discloses restricting such traffic based on, for example, a time of day or size of attachments. EX1017, ¶26. A POSITA would have been motivated to implement *Weintraub*'s restriction settings based on network traffic

classification to manage bandwidth usage in the *Thomas-Buddhikot* hotspot device. EX1003, ¶148. For example, during times of high demand (e.g., during the day) a POSITA would have been motivated to restrict network traffic associated with VOIP or large email attachments because this traffic consumes available bandwidth and leaves less bandwidth for all the users. EX1003, ¶148.

Implementing *Weintraub*'s teaching of limiting traffic based on a network traffic classification on the *Thomas-Buddhikot* hotspot device would have been a combination of familiar elements (e.g., rules for limiting bandwidth based on classification) according to known methods (e.g., implementing additional traffic control rules providing in the *Thomas-Buddhikot* hotspot device) to obtain predictable results (e.g., ensuring client devices connected to the *Thomas-Buddhikot* hotspot device can exchange data with a minimum bandwidth).

EX1003, ¶149; *KSR*, 550 U.S. at 416. A POSITA would have had a reasonable expectation of success in implementing *Weintraub*'s teaching of limiting traffic based on a network traffic classification on the *Thomas-Buddhikot* hotspot device.

EX1003, ¶149. *Thomas* already discloses rules for controlling traffic through its hotspot device. EX1005, ¶¶68-69. The *Thomas-Buddhikot* combination also already teaches or suggests techniques for implementing additional firewalling and packet-mangling rules on the *Thomas-Buddhikot* hotspot device. *Supra* §VI.A.2.d. Thus, implementing *Weintraub*'s rules for restricting traffic based on network

classification on the *Thomas-Buddhikot* hotspot device would have involved known techniques as disclosed by *Thomas*, *Buddhikot*, and *Weintraub* and would have been well within the skill level of a POSITA. EX1003, ¶149. Accordingly, a POSITA would have had a reasonable expectation of success in combining *Weintraub*'s teachings with the *Thomas-Buddhikot* hotspot device. EX1003, ¶149.

b. Parental control policy

Weintraub discloses policies that allow a parent to restrict adult content from devices associated with young children in the household. EX1017, ¶10. A POSITA would have been motivated to implement such parental control policies on the *Thomas-Buddhikot* hotspot device to achieve the same benefits, namely to allow parents to restrict inappropriate content (e.g., adult content unsuitable for children) from being forwarded by the *Thomas-Buddhikot* hotspot device to the children's end point devices. Implementing *Weintraub*'s teaching of restricting content based on a parental control policy on the *Thomas-Buddhikot* hotspot device would have been a combination of familiar elements (rules for restricting content based on type of content) according to known methods (e.g., implementing additional traffic control rules providing in the *Thomas-Buddhikot* hotspot device) to obtain predictable results (e.g., inappropriate adult content is not delivered to children's end point devices). EX1003, ¶150; *KSR*, 550 U.S. at 416.

A POSITA would have had a reasonable expectation of success in implementing *Weintraub*'s teaching of restricting content based on a parental control policy on the *Thomas-Buddhikot* hotspot device. EX1003, ¶151. *Thomas* already discloses rules for controlling traffic through its hotspot device. EX1005, ¶¶68-69. The *Thomas-Buddhikot* combination already teaches or suggest techniques for implementing additional firewalling and packet-mangling rules on the *Thomas-Buddhikot* hotspot device. *Supra* §VI.A.2.d. Thus, implementing *Weintraub*'s rules restricting traffic based on network classification on the *Thomas-Buddhikot* hotspot device would have involved known techniques as disclosed by *Thomas*, *Buddhikot*, and *Weintraub* and would have been well within the skill level of a POSITA. EX1003, ¶151. Accordingly, a POSITA would have had a reasonable expectation of success in combining *Weintraub*'s teachings with *Thomas* and *Buddhikot*. EX1003, ¶151.

2. Claims 35 and 48:

a. Claim 35: “The network system of claim 34, wherein the one or more restriction settings includes restriction settings that vary depending on a network traffic classification of the data.”

Claim 35 depends from claim 34, which would have been obvious as discussed above. *Supra* §VI.A.11. The *Thomas-Buddhikot-Weintraub* combination discloses the additional features of claim 35. EX1003, ¶152. *Weintraub* discloses

different restriction settings based on a network traffic classification. EX1017, ¶26. For example, *Weintraub* discloses that “[p]olicies may also be defined, for example, for instant messaging (e.g., to restrict instant messaging based on time of day, based on the IM destination (or origination), based on the content of an instant message, etc.), Voice over IP (e.g., SIP) communications (e.g., to restrict communications based on source/destination, time of day, domain, etc.), peer-to-peer transmissions (e.g., to restrict transmissions based on source/destination, etc.), e-mail transmissions (e.g., to restrict transmissions based on source/destination, time of day, attachments, words in the e-mail transmissions, etc.), streaming media (e.g., to restrict media based on time of day, ratings, etc.), and/or other types of traffic.” EX1017, ¶26.

A POSITA would have understood that implementing *Weintraub*’s teachings on the *Thomas-Buddhikot* hotspot device would allow it to restrict traffic based on a network classification such as type of data (e.g., instant messaging, voice over IP, peer-to-peer transmissions, email transmissions, streaming media transmissions) at particular times of day, to ensure sufficient bandwidth is available to all users. EX1003, ¶153. As explained above, a POSITA would have found it obvious to combine the teachings of *Thomas*, *Buddhikot*, and *Weintraub*. *Supra* §VI.D.1.a.

b. Claim 48: “The method of claim 44, wherein the one or more restriction settings include restriction settings that vary depending on a network traffic classification of the data.”

Claim 48 depends from claim 44, which would have been obvious as discussed above. *Supra* §VI.A.16. The *Thomas-Buddhikot-Weintraub* combination discloses the additional features of claim 48 for the same reasons as those described above for claim 35. *Supra* §VI.D.3.a; EX1003, ¶¶154-56.

3. Claims 37, 38, 46, and 47

a. Claim 37: “The network system of claim 24, wherein a particular restriction setting restricts data associated with certain network destinations from the access network forwarding service.”

Claim 37 depends from claim 24, which would have been obvious as discussed above. *Supra* §VI.A.2. The *Thomas-Buddhikot-Weintraub* combination discloses the additional features of claim 37. EX1003, ¶157. As explained for 24[pre][iii], in the *Thomas-Buddhikot* hotspot device, the firewall service is configured to use packet-mangling rules to protect the *Thomas-Buddhikot* hotspot device and/or client devices connected to the *Thomas-Buddhikot* hotspot device from malicious attacks. *Supra* §VI.A.2.d. *Weintraub* further discloses policies that prohibit a customer device within the customer’s premises from accessing adult content from the external network. EX1017, ¶10. A POSITA would have understood that implementing *Weintraub*’s teachings on the *Thomas-Buddhikot*

hotspot device would allow it to restrict traffic based on a parental control policy by prohibiting data related to adult content from being delivered to a client device connected to the *Thomas-Buddhikot* hotspot device. EX1003, ¶157; *compare with* EX1001 18:32-52 (describing “firewall function” that blocks device access to network destinations when service usage is out of policy). As explained, a POSITA would have found it obvious to combine the teachings of *Thomas*, *Buddhikot*, and *Weintraub*. *Supra* §VI.D.1.b.

b. Claim 38: “The network system of claim 37, wherein the network destinations that are restricted are determined by a parental control policy.”

Claim 38 depends from claim 37, which would have been obvious as discussed above. *Supra* §VI.D.3.a. The *Thomas-Buddhikot-Weintraub* combination discloses the additional features of claim 38. EX1003, ¶158. For example, *Weintraub* discloses restriction settings based on a parental control policy. EX1017, ¶11. For example, *Weintraub* discloses policies that prohibit a customer device within the customer’s premises from accessing adult content from the external network. EX1017, ¶10. According to *Weintraub*, “[w]hen traffic containing adult content is received from the external network . . . the policy enforcement point may stop the traffic (e.g., by discarding it) prior to reaching the customer device.” EX1017, ¶10, Fig. 1. *Weintraub* explains that “[t]he customers premises may refer to a household where a parent wishes to control, via the

policies, the content that may be provided to his/her children or access to communications.” EX1017, ¶11.

A POSITA would have understood that implementing *Weintraub*’s teachings on the *Thomas-Buddhikot* hotspot device would allow it to restrict traffic based on a parental control policy by prohibiting data related to adult content from being delivered to a client device connected to the *Thomas-Buddhikot* hotspot device. EX1003, ¶159. As explained, a POSITA would have found it obvious to combine the teachings of *Thomas*, *Buddhikot*, and *Weintraub*. *Supra* §VI.D.1.b.

c. Claim 46: “The method of claim 44, wherein a particular restriction setting restricts data associated with certain network destinations from the access network forwarding service.”

Claim 46 depends from claim 44, which would have been obvious as discussed above. *Supra* §VI.A.16. The *Thomas-Buddhikot* combination discloses claim 46 for the same reasons as claim 37. *Supra* §VI.D.3.a; EX1003, ¶¶160-61.

d. Claim 47: “The method of claim 46, wherein the network destinations that are restricted are determined by a parental control policy.”

Claim 47 depends from claim 46, which would have been obvious as discussed above. *Supra* §. The *Thomas-Buddhikot-Weintraub* combination discloses the additional features of claim 46 for the same reasons as claim 38. *Supra* §VI.D.3.b; EX1003, ¶¶162-64.

VII. Mandatory Notices

A. Real Parties-in-Interest

Google LLC² is a real party-in-interest.

Out of an abundance of caution, Google identifies Apple Inc. (“Apple”) as a real party-in-interest. Apple and Headwater have recently entered into “a worldwide settlement whereby Headwater licensed its patents to Apple.” Patent Owner’s Request for Discretionary Denial of Institution, *Google LLC v. Headwater Research LLC*, IPR2026-00048, Paper 8, 2 (PTAB Jan. 7, 2026).

As identified in the related matters below, the ’425 patent is being asserted against multiple Carriers in 2:25-cv-00914, 2:25-cv-00919, and 2:25-cv-00921. On December 1, 2025, the Carriers in those cases filed a joint opposed motion to stay the litigations under, among other things, the customer-suit exception. *See* Defendants’ Joint Opposed Motion to Stay, *Headwater Res. LLC v. DISH Network Corp.*, 2:25-cv-00921 (Dec. 1, 2025), ECF No. 52. On December 8, 2025, a redacted version of that motion was made publicly available. *See id.* ECF No. 63. On December 19, 2025, Headwater filed a sealed response to the motion. *See id.* ECF No. 73. On January 9, 2026, the Carriers filed a sealed reply. *See id.* ECF No.

² Google LLC is a subsidiary of XXVI Holdings Inc., which is a subsidiary of Alphabet Inc.

82. In light of these filings, Google names the following Carriers (the named defendants in these cases) as real parties-in-interest to this proceeding:

- DISH Network Corporation f/k/a EchoStar Communications Corporation
- DISH Network LLC
- Dish Wireless, LLC d/b/a Boost Mobile
- Charter Communications, Inc.
- Charter Communications, LLC
- Charter Communications Operating, LLC
- Comcast Cable Communications, LLC d/b/a Xfinity
- Comcast Cable Communications Management, LLC
- Comcast Corporation
- Comcast of Houston, LLC d/b/a Xfinity
- Spectrum Gulf Coast, LLC
- Spectrum Management Holding Company, LLC

Charter Communications, Inc., Charter Communications, LLC, Charter Communications Operating, LLC, Spectrum Gulf Coast, LLC, Spectrum Management Holding Company, LLC and Headwater Research LLC filed a Joint Motion to Stay All Deadlines and Notice of Settlement on August 5, 2026. *See id.* ECF No. 110.

Comcast Cable Communications, LLC d/b/a Xfinity, Comcast Cable Communications Management, LLC, Comcast of Houston, LLC, and Headwater Research LLC filed a Joint Motion to Stay All Deadlines and Notice of Settlement on August 7, 2026. *See id.* ECF No. 112.

To be clear, none of these Carriers funded, directed, or controlled the filing or preparation of this petition, nor did Google prepare or file the petition at the Carriers' behest. Instead, Google makes this identification out of an abundance of caution and in the interest of over-disclosure.

B. Related Matters

The '425 patent is or has been involved in the following proceedings:

Name	Number	Forum	Filed
<i>Google LLC v. Headwater Research LLC</i>	IPR2026-00464	P.T.A.B.	Aug. 28, 2026
<i>Headwater Research LLC v. Comcast Cable Communications, LLC d/b/a Xfinity et al</i>	2:25-cv-00914	E.D. Tex.	Aug. 29, 2025
<i>Headwater Research LLC v. Charter Communications, Inc. et al</i>	2:25-cv-00919	E.D. Tex.	Aug. 29, 2025
<i>Headwater Research LLC v. DISH Network Corporation et al</i>	2:25-cv-00921	E.D. Tex.	Aug. 29, 2025
<i>Headwater Research LLC v. Apple Inc.</i>	7:25-cv-00375	W.D. Tex.	Aug. 27, 2025
<i>Headwater Research LLC v. Google LLC</i>	7:25-cv-00376	W.D. Tex.	Aug. 27, 2025
<i>Headwater Research LLC v. AT&T Inc. et al</i>	2:25-cv-00428	E.D. Tex.	Apr. 23, 2025

<i>Headwater Research LLC v. Cellco Partnership, d/b/a Verizon Wireless et al</i>	2:25-cv-00391	E.D. Tex.	Apr. 15, 2025
<i>Headwater Research LLC v. Sprint LLC et al</i>	2:25-cv-00359	E.D. Tex.	Apr. 8, 2025

C. Lead and Back-Up Counsel

Lead Counsel	Back-Up Counsel
Erika H. Arner, Reg. No. 57,540 erika.arner@finnegan.com Finnegan, Henderson, Farabow, Garrett, & Dunner LLP 1875 Explorer Street, Suite 800 Reston, VA 20190-6023 Tel: 571-203-2754 Fax: 202-408-4400	Joshua L. Goldberg, Reg. No. 59,369 joshua.goldberg@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 901 New York Avenue NW Washington, DC 20001-4413 Phone: 202-408-6092 Fax: 202-408-4400 Daniel C. Tucker, Reg. No. 62,781 daniel.tucker@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 1875 Explorer St, Suite 800 Reston, VA 20190-6023 Tel: 571-203-2793 Fax: 202-408-4400 Benjamin A. Saidman, Reg. No. 69,325 benjamin.saidman@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 271 17th Street NW, Suite 1400 Atlanta, GA 30363-6209 Phone: 404-653-6510 Fax: 404-653-6444 Daniel F. Klodowski, Reg. No. 72,693 daniel.klodowski@finnegan.com

Lead Counsel	Back-Up Counsel
	Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 901 New York Avenue NW Washington, DC 20001-4413 Phone: 202-408-4216 Fax: 202-408-4400 Elliot Cook, Reg No. 61,769 elliot.cook@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 1875 Explorer St, Suite 800 Reston, VA 20190-6023 Tel: 571-203-2738 Fax: 202-408-4400 Michael V. Young (Reg. No. 61,180) michael.young@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 1875 Explorer Street, Suite 800 Reston, VA 20190-6023 Phone: 571-203-2788 Fax: 202-408-4400 Alexander M. Boyer, Reg. No. 66,599 alexander.boyer@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 1875 Explorer Street, Suite 800 Reston, VA 20190-6023 Phone: 571-203-2759 Fax: 202-408-4400 Pier D. DeRoo, Reg. No. 69,340 pier.deroo@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP

Lead Counsel	Back-Up Counsel
	901 New York Avenue NW Washington, DC 20001-4413 Phone: 202-408-4418 Fax: 202-408-4400 Christopher C. Johns, Reg. No. 68,664 Christopher.Johns@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 901 New York Avenue NW, Washington, DC 20001-4413 Tel: 202-408-4155 Fax: 202-408-4400 Kassandra M. Officer, Reg. No. 74,083 Kassandra.Officer@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 901 New York Avenue NW, Washington, DC 20001-4413 Tel: 202-408-4270 Fax: 202-408-4400 Bradford C. Schulz, Reg. No. 75,006 bradford.schulz@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 1875 Explorer Street, Suite 800 Reston, VA 20190-6023 Tel: 571-203-2739 Fax: 202-408-4400 William C. Neer, Reg. No. 78,874 Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 901 New York Avenue NW Washington, DC 20001-4413 Phone: 202-408-4054

Lead Counsel	Back-Up Counsel
	Fax: 202-408-4400 Christopher B. Anderson, Reg. No. 77,898 christopher.anderson@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 1875 Explorer St, Suite 800 Reston, VA 20190-6023 Tel: 571-203-2765 Fax: 202-408-4400 Kai Rajan, Reg. No. 70,110 kai.rajan@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 901 New York Avenue NW Washington, DC 20001-4413 Phone: 202-408-4363 Fax: 202-408-4400 Umber Aggarwal, Reg. No. 76,098 umber.aggarwal@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 1875 Explorer Street, Suite 800 Reston, VA 20190-6023 Tel: 571-203-2423 Fax: 202-408-4400 Abhay A. Watwe, Reg. No. 59,461 abhay.watwe@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 1875 Explorer Street, Suite 800 Reston, VA 20190-6023 Tel: 571-203-2716 Fax: 202-408-4400

Lead Counsel	Back-Up Counsel
	Kathleen C. Galleher, Reg. No. 80,837 kathleen.galleher@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 1875 Explorer Street, Suite 800 Reston, VA 20190-6023 Tel: 571-203-2448 Fax: 202-408-4400 Connor M. McGregor, Reg. No. 79,634 connor.mcgregor@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 901 New York Avenue NW Washington, DC 20001-4413 Phone: 202-408-4363 Fax: 202-408-4400 Heather J. Ren, Reg. No. 82,089 heather.ren@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 901 New York Avenue NW Washington, DC 20001-4413 Phone: 202-408-4024 Fax: 202-408-4400 Yi Yang, <i>pro hac vice</i> to be filed yi.yang@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 2 Seaport Lane, 6th Floor Boston, MA 02210 Phone: 617-646-1642 Fax: 202-408-4400

D. Service Information

Petitioner consents to being served electronically at the e-mail addresses provided above and at HeadwaterIPRTeam@finnegan.com.

VIII. Grounds for Standing

Petitioner certifies that the '425 patent is available for IPR and that Petitioner is not barred or estopped from requesting IPR challenging the patent claims on the grounds in this Petition.

IX. Conclusion

Petitioner requests IPR and cancellation of claims 24-50. The Office may charge any required fees to Deposit Account No. 06-0916.

Date: August 28, 2026

Respectfully submitted,

By: /Erika H. Arner/
Erika H. Arner, Lead Counsel
Reg. No. 57,540

CERTIFICATION OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24, Petitioner certifies that the word count of Petitioner's Petition for *Inter Partes* Review (exclusive of any table of contents, table of authorities, mandatory notices under § 42.8, certificates of service and word count, and list of exhibits or claim listing) as measured by Microsoft Word is 13,259.

Dated: August 28, 2026

By: /Erika H. Arner/
Erika H. Arner, Lead Counsel
Reg. No. 57,540

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(a), the undersigned certifies that on August 28, 2026, a copy of the foregoing Petition for *Inter Partes* Review, the associated power of attorney, and Exhibits 1001-1005, 1013, 1015-1018, 1025 were served by FedEx Priority Overnight on the correspondence address of record indicated in the Patent Office's Patent Center website for U.S. Patent No. 8,023,425:

James Harris
Headwater Research LLC - Outside Firm 1
110 North College Avenue
Suite 1116
Tyler, TX 75702
UNITED STATES

Date: August 28, 2026

By: /Lisa C. Hines/
Lisa C. Hines
Case Manager
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, LLP